



Manual do usuário

AWS Site-to-Site VPN



AWS Site-to-Site VPN: Manual do usuário

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o Site-to-Site VPN	1
Conceitos	1
Recursos da Site-to-Site VPN	2
Limitações do Site-to-Site VPN	2
Trabalhar com Site-to-Site VPN	3
Definição de preço	3
Como AWS Site-to-Site VPN funciona	4
Gateway privado virtual	4
Transit gateway	5
Dispositivo de gateway do cliente	5
Gateway do cliente	6
Opções de túnel VPN	6
Opções de autenticação de túnel VPN	13
Chaves pré-compartilhadas	13
Certificado privado de AWS Private Certificate Authority	13
Opções de iniciação do túnel da VPN	14
Opções de iniciação do protocolo IKE de túnel da VPN	14
Regras e limitações	15
Trabalhar com opções de iniciação de túnel da VPN	15
Substituições de endpoint	16
Substituições de endpoint iniciadas pelo cliente	16
Substituições de endpoints gerenciados pela AWS	17
Ciclo de vida do endpoint de túnel	17
Opções de gateway do cliente	23
Conexões VPN aceleradas	25
Habilitar a aceleração	26
Regras e restrições	26
Opções de roteamento site a VPN site	27
Roteamento estático e dinâmico	28
Tabelas de rotas e prioridade de VPN rotas	28
Roteamento durante atualizações do endpoint VPN do túnel	31
Tráfego IPv4 e IPv6	31
Tutorial de inicialização	33
Pré-requisitos	33

Criar um gateway do cliente	35
Criar um gateway de destino	36
Criar um gateway privado virtual	36
Criar um gateway de trânsito	37
Configurar o roteamento	37
(Gateway privado virtual) Habilitar a propagação de rotas na tabela de rotas	37
(Gateway de trânsito) Adicionar uma rota à tabela de rotas	39
Atualizar o grupo de segurança	39
Criar uma conexão VPN	40
Baixar arquivo de configuração	41
Configurar o dispositivo de gateway do cliente	43
Arquiteturas	44
Vários cenários VPN de conexão	44
Conexões VPN única e múltipla	45
AWS VPN CloudHub	50
Conexões VPN redundantes	52
O dispositivo de gateway do cliente	55
Requisitos	56
Práticas recomendadas	59
Regras de firewall	61
Exemplo de arquivos de configuração	64
Exemplo de configurações para roteamento estático	66
Exemplo de configurações para roteamento dinâmico	80
Configurar o Windows Server como um dispositivo de gateway do cliente	92
Configurar a instância do Windows	92
Etapa 1: Criar uma conexão VPN e configurar a VPC	93
Etapa 2: Fazer download do arquivo de configuração para a conexão VPN	94
Etapa 3: configurar o Windows Server	97
Etapa 4: Configurar o túnel VPN	98
Etapa 5: Habilitar a detecção de gateway inativo	105
Etapa 6: Testar a conexão VPN	105
Solução de problemas	106
Dispositivo com BGP	107
Dispositivo sem BGP	110
Cisco ASA	113
Cisco IOS	117

Cisco IOS sem BGP	123
Juniper JunOS	129
Juniper ScreenOS	134
Yamaha	137
Trabalhar com o Site-to-Site VPN	142
Crie um anexo VPN para AWS Cloud WAN	142
Criar um anexo de VPN do gateway de trânsito	144
Testar uma conexão VPN	146
Excluir uma conexão VPN	147
Excluir uma conexão VPN	148
Excluir um gateway do cliente	148
Desanexar e excluir um gateway privado virtual	149
Modificar o gateway de destino de uma conexão VPN	150
Etapa 1: Criar o gateway de destino	151
Etapa 2: excluir as rotas estáticas (condicional)	151
Etapa 3: Migrar para um novo gateway	152
Etapa 4: Atualizar tabelas de rotas da VPC	152
Etapa 5: Atualizar o roteamento do gateway de destino (condicional)	153
Etapa 6: atualizar o ASN do gateway do cliente (condicional)	154
Modificar opções da conexão VPN	154
Modificar opções de túnel da VPN	155
Editar rotas estáticas para uma conexão VPN	156
Alterar o gateway do cliente para uma conexão VPN	157
Substituir credenciais comprometidas	157
Alternar os certificados de endpoint do túnel da VPN	158
VPN IP privada com AWS Direct Connect	159
Benefícios da VPN de IP privado	159
Como funciona a VPN de IP privado	160
Pré-requisitos	160
Criar o gateway do cliente	161
Preparar o gateway de trânsito	161
Crie o AWS Direct Connect gateway	162
Criar a associação a um gateway de trânsito	162
Criar a conexão VPN	163
Segurança	165
Proteção de dados	165

Privacidade do tráfego entre redes	167
Gerenciamento de identidade e acesso	167
Público	168
Autenticando com identidades	169
Gerenciando acesso usando políticas	172
Como funciona AWS o site a site com VPN IAM	175
Exemplos de políticas baseadas em identidade	182
Solução de problemas	185
Usar funções vinculadas ao serviço	187
Resiliência	189
Dois túneis por conexão VPN	190
Redundância	190
Segurança da infraestrutura	190
Monitorar a conexão do Site-to-Site VPN	192
Ferramentas de monitoramento	193
Ferramentas de monitoramento automatizadas	193
Ferramentas de monitoramento manual	193
AWS Site-to-Site VPN troncos	194
Benefícios dos logs do Site-to-Site VPN	195
Restrições de tamanho da política de recursos do Amazon CloudWatch Logs	195
Conteúdo dos logs do Site-to-Site VPN	196
Requisitos do IAM para publicar no CloudWatch Logs	199
Exibir configuração de logs do Site-to-Site VPN	200
Habilitar os logs do Site-to-Site VPN	201
Desabilitar logs do Site-to-Site VPN	202
Monitoramento de túneis VPN usando a Amazon CloudWatch	203
Métricas e dimensões da VPN	203
Visualizando CloudWatch métricas de VPN	205
Criação de CloudWatch alarmes para monitorar túneis VPN	205
Monitoramento de conexões VPN usando AWS Health eventos	208
Notificações de substituição de endpoint do túnel	209
Notificações de VPN de túnel único	209
Cotas	210
Recursos do Site-to-Site VPN	210
Rotas	211
Largura de banda e taxa de transferência	212

A unidade de transmissão máxima (MTU)	212
Recursos de cota adicionais	213
Histórico do documento	214
.....	ccxix

O que AWS Site-to-Site VPN é

Por padrão, as instâncias executadas na Amazon VPC não podem comunicar-se com sua própria rede (remota). Você pode habilitar o acesso à sua rede remota pela VPC criando uma conexão AWS Site-to-Site VPN (Site-to-Site VPN) e configurando o roteamento para transmitir o tráfego pela conexão.

O termo conexão VPN possui sentido amplo, mas, nesta documentação, ele se refere especificamente à conexão entre a VPC e sua rede local. A VPN de local para local oferece suporte para as conexões VPN da Internet Protocol security (IPsec).

Conteúdo

- [Conceitos](#)
- [Recursos da Site-to-Site VPN](#)
- [Limitações do Site-to-Site VPN](#)
- [Trabalhar com Site-to-Site VPN](#)
- [Definição de preço](#)

Conceitos

Veja a seguir os principais conceitos do Site-to-Site VPN:

- **Conexão VPN:** uma conexão segura entre seu equipamento no local e suas VPCs.
- **Túnel VPN:** um link criptografado em que os dados podem transmitir da rede do cliente para a AWS ou vice-versa.

Cada conexão VPN inclui dois túneis VPN que podem ser usados simultaneamente para alta disponibilidade.

- **Gateway do cliente:** um AWS recurso que fornece informações AWS sobre seu dispositivo de gateway do cliente.
- **Gateway do cliente:** é um dispositivo físico ou aplicação de software situada no seu lado da conexão do Site-to-Site VPN.
- **Gateway de destino:** um termo genérico para o endpoint da VPN no lado da Amazon da conexão VPN Site-to-Site.

- **Gateway privado virtual:** um gateway privado virtual é o endpoint da VPN situado no lado da Amazon de sua conexão VPN Site-to-Site que pode ser anexado a uma única VPC.
- **Gateway de trânsito:** um hub de trânsito que pode ser usado para interconectar várias VPCs e redes on-premises e como um endpoint de VPN para o lado da Amazon da conexão VPN Site-to-Site.

Recursos da Site-to-Site VPN

Os seguintes recursos são compatíveis com AWS Site-to-Site VPN conexões:

- Internet Key Exchange versão 2 (IKEv2)
- NAT Traversal
- ASN de 4 bytes no intervalo de 1 a 2147483647 para configuração do Gateway Privado Virtual (VGW). Consulte [Opções de gateway do cliente para a conexão de VPN de local a local](#) para obter mais informações.
- ASN de 2 bytes para CGW (Gateway do Cliente) na faixa de 1 a 65535. Consulte [Opções de gateway do cliente para a conexão de VPN de local a local](#) para obter mais informações.
- CloudWatch métricas
- Endereços IP reutilizáveis para os gateways do cliente
- Opções de criptografia adicionais; incluindo criptografia AES de 256 bits, hashing SHA-2 e grupos Diffie-Hellman adicionais
- Opções de túnel configuráveis
- ASN privado do cliente para o lado da Amazon de uma sessão BGP
- Certificado privado de uma CA subordinada de AWS Private Certificate Authority
- Suporte a tráfego IPv6 para conexões VPN em um gateway de trânsito.

Limitações do Site-to-Site VPN

Uma conexão do Site-to-Site VPN tem as seguintes limitações.

- O tráfego IPv6 não é compatível com conexões VPN em um gateway privado virtual.
- Uma AWS VPN conexão não oferece suporte ao Path MTU Discovery.

Além disso, leve o seguinte em consideração ao usar o Site-to-Site VPN:

- Ao conectar suas VPCs a uma rede local comum, recomendamos que você use blocos CIDR não sobrepostos nas redes.

Trabalhar com Site-to-Site VPN

Você pode criar, acessar e gerenciar seus recursos do Site-to-Site VPN usando qualquer uma das seguintes interfaces:

- AWS Management Console: fornece uma interface da Web que pode ser usada para acessar os recursos do Site-to-Site VPN.
- AWS Command Line Interface (AWS CLI) — Fornece comandos para um amplo conjunto de AWS serviços, incluindo Amazon VPC, e é compatível com Windows, macOS e Linux. Para ter mais informações, consulte [AWS Command Line Interface](#).
- AWS SDKs — fornecem APIs específicas do idioma e cuidam de muitos detalhes da conexão, como calcular assinaturas, lidar com novas tentativas de solicitação e tratamento de erros. Para obter mais informações, consulte [AWS SDKs](#).
- API de consulta: fornece ações de API de baixo nível que são chamadas usando solicitações HTTPS. Usar a API de consulta é a maneira mais direta para acessar a Amazon VPC, mas exige que a aplicação lide com detalhes de baixo nível, como geração de hash para assinar a solicitação e tratamento de erros. Para obter mais informações, consulte a [Referência de API do Amazon EC2](#).

Definição de preço

Você é cobrado por cada hora de conexão VPN em que a sua conexão VPN é provisionada e disponível. Para obter mais informações, consulte [Definição de preço da conexão VPN Site-to-Site AWS Site-to-Site VPN](#).

Você é cobrado pela transferência de dados do Amazon EC2 para a Internet. Para obter mais informações, consulte a seção [Data Transfer](#) (Transferência de dados) na página On-Demand Pricing do Amazon EC2 (Definição de preço sob demanda do Amazon EC2).

Quando você cria uma conexão VPN acelerada, criamos e gerenciamos dois aceleradores em seu nome. Você é cobrado por uma taxa horária e custos de transferência de dados para cada acelerador. Para obter mais informações, consulte [Preços do AWS Global Accelerator](#).

Como AWS Site-to-Site VPN funciona

Uma conexão do Site-to-Site VPN possui os seguintes componentes:

- Um [gateway privado virtual](#) ou um [gateway de trânsito](#)
- Um [dispositivo de gateway do cliente](#)
- Um [gateway do cliente](#)

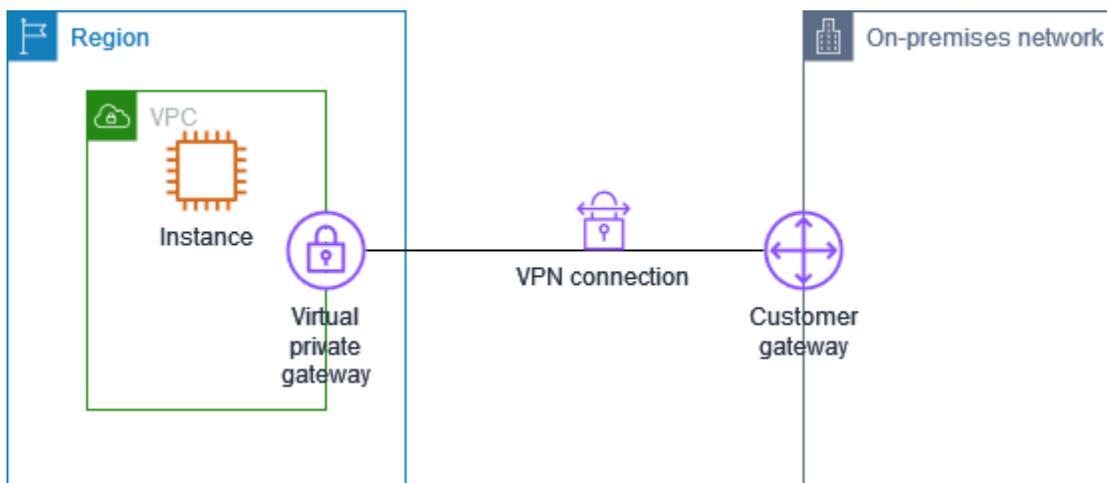
A conexão VPN oferece dois túneis VPN entre um gateway privado virtual ou gateway de trânsito no AWS lado e um gateway de cliente no lado local.

Para obter mais informações sobre cotas de Site-to-Site VPN, consulte [Cotas do Site-to-Site VPN](#).

Gateway privado virtual

Um gateway privado virtual é o concentrador VPN situado no lado da Amazon de uma conexão do Site-to-Site VPN. Você cria um gateway privado virtual e o anexa a uma nuvem privada virtual (VPC) com recursos que devem acessar a conexão do Site-to-Site VPN.

O diagrama a seguir mostra uma conexão VPN entre uma VPC e a rede on-premises usando um gateway privado virtual.



Quando você cria um gateway privado virtual, é possível especificar o Número de sistema autônomo privado (ASN) para o lado da Amazon do gateway. Se você não especificar um ASN, o gateway privado virtual é criado com o ASN (64512) padrão. Você não poderá alterar o ASN depois de ter criado o gateway privado virtual. Para verificar o ASN do seu gateway privado virtual, veja seus

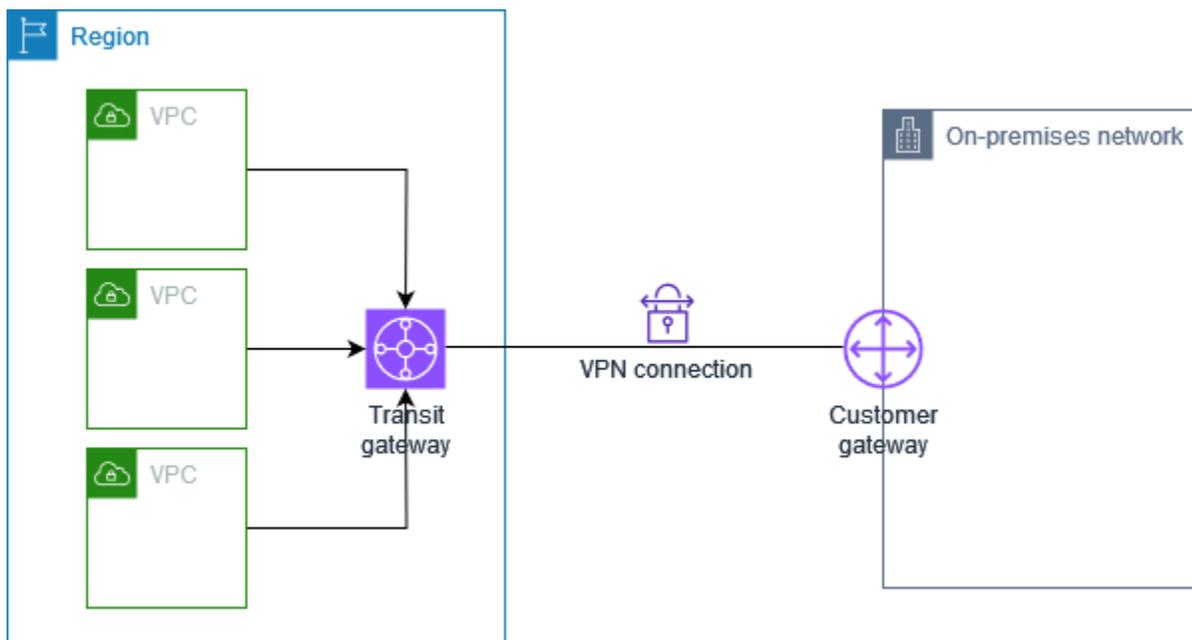
detalhes na página Gateways privados virtuais no console da Amazon VPC ou use o comando.

[describe-vpn-gateways](#) AWS CLI

Transit gateway

Um gateway de trânsito é um hub de trânsito que pode ser usado para interconectar as VPCs e as redes on-premises. Para obter mais informações, consulte [Gateways de trânsito da Amazon VPC](#). Você pode criar uma conexão do Site-to-Site VPN como um anexo em um gateway de trânsito.

O diagrama a seguir mostra uma conexão VPN entre várias VPCs e a rede on-premises usando um gateway de trânsito. O gateway de trânsito tem três anexos de VPC e um anexo de VPN.



A conexão do Site-to-Site VPN em um gateway de trânsito pode ser compatível com tráfego IPv4 ou IPv6 dentro dos túneis VPN. Para ter mais informações, consulte [Tráfego IPv4 e IPv6](#).

É possível modificar o gateway de destino de uma conexão do Site-to-Site VPN de um gateway privado virtual a um gateway de trânsito. Para obter mais informações, consulte [the section called “Modificar o gateway de destino de uma conexão VPN”](#).

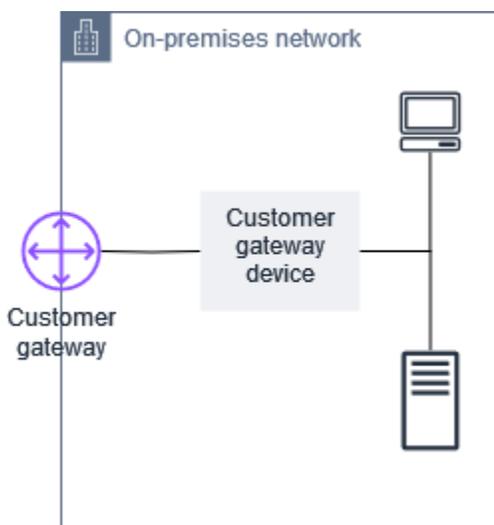
Dispositivo de gateway do cliente

Um dispositivo gateway do cliente é um dispositivo físico ou aplicativo de software no seu lado da conexão do Site-to-Site VPN. Configure o dispositivo para funcionar com a conexão do Site-to-Site VPN. Para obter mais informações, consulte [O dispositivo de gateway do cliente](#).

Por padrão, o dispositivo de gateway do cliente deve ativar os túneis para a conexão do Site-to-Site VPN gerando tráfego e iniciando o processo de negociação do protocolo IKE. Em vez disso, você pode configurar a conexão da VPN de local a local para especificar que a AWS deve iniciar o processo de negociação do IKE. Para obter mais informações, consulte [Opções de iniciação de túnel do Site-to-Site VPN](#).

Gateway do cliente

Um gateway do cliente é um recurso que você cria na AWS e representa o dispositivo de gateway do cliente na rede local. Ao criar um gateway do cliente, você fornece informações sobre seu dispositivo para AWS. Para ter mais informações, consulte [the section called “Opções de gateway do cliente”](#).

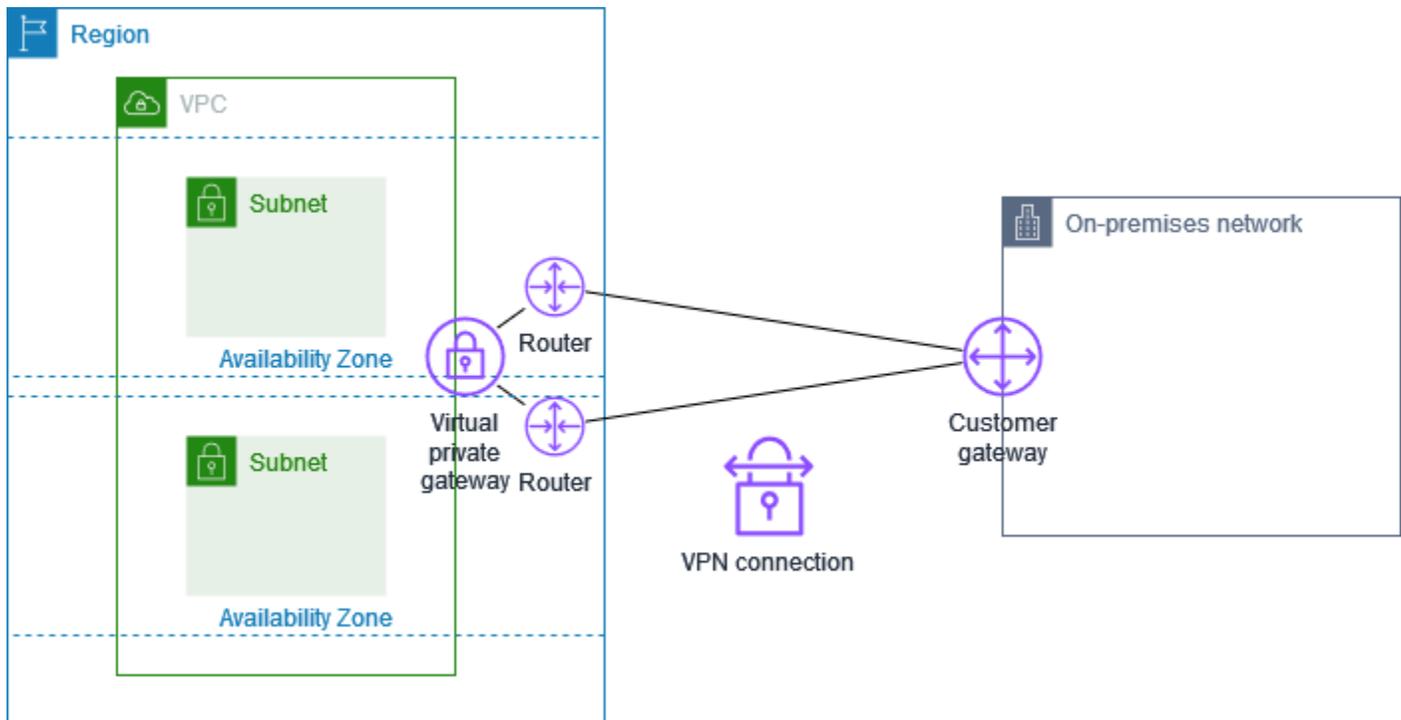


Para usar a Amazon VPC com uma conexão do Site-to-Site VPN, você ou o administrador da rede também deverá configurar o dispositivo ou aplicativo do gateway do cliente na rede remota. Quando você cria a conexão do Site-to-Site VPN, fornecemos as informações de configuração necessárias e o administrador da rede geralmente executa a configuração. Para obter informações sobre os requisitos e a configuração do gateway do cliente, consulte [O dispositivo de gateway do cliente](#).

Opções de túnel para a conexão do Site-to-Site VPN

Use uma conexão do Site-to-Site VPN para conectar a rede remota a uma VPC. Cada conexão da VPN local a local tem dois túneis, sendo que cada um usa um endereço IP público exclusivo. Para a redundância, é importante configurar ambos os túneis. Quando um túnel fica indisponível (por exemplo, para manutenção), o tráfego de rede é roteado automaticamente para o túnel que estiver disponível para aquela conexão do Site-to-Site VPN específica.

O diagrama a seguir mostra os dois túneis de uma conexão VPN. Cada túnel termina em uma zona de disponibilidade diferente para fornecer maior disponibilidade. Tráfego da rede local para AWS usar os dois túneis. O tráfego AWS para a rede local prefere um dos túneis, mas pode passar automaticamente para o outro túnel se houver uma falha lateral. AWS



Ao criar uma conexão do Site-to-Site VPN, fazer download de um arquivo de configuração específico para seu dispositivo de gateway do cliente que contém informações para configuração do dispositivo, incluindo as informações para configuração de cada túnel. Como opção, você mesmo pode especificar algumas das opções de túnel ao criar a conexão do Site-to-Site VPN. Caso contrário, a AWS fornece os valores padrão.

Note

Os endpoints do túnel da VPN de local para local avaliam as propostas do gateway do cliente começando com o menor valor configurado da lista abaixo, independentemente da ordem da proposta do gateway do cliente. Você pode usar o `modify-vpn-connection-options` comando para restringir a lista de opções que os AWS endpoints aceitarão. Para obter mais informações, consulte a [modify-vpn-connection-options](#) Referência de linha de comando do Amazon EC2.

Veja a seguir as opções de túnel que você pode configurar.

Tempo limite do Dead Peer Detection (DPD)

A duração, em segundos, após a qual ocorre o tempo limite do DPD. Um tempo limite do DPD de 40 segundos significa que o endpoint da VPN considerará o par desativado 30 segundos após a primeira falha no keep-alive. Você pode especificar 30 ou superior.

Padrão: 60

Ação de tempo limite do DPD

A ação a ser executada após atingir o tempo limite do Dead Peer Detection (DPD). Você pode especificar o seguinte:

- **Clear**: finalizar a sessão do protocolo IKE quando o tempo limite do DPD for atingido (interromper o túnel e limpar as rotas)
- **None**: nenhuma ação quando o tempo limite do DPD for atingido
- **Restart**: reiniciar a sessão do protocolo IKE quando o tempo limite do DPD for atingido

Para obter mais informações, consulte [Opções de iniciação de túnel do Site-to-Site VPN](#).

Padrão: **Clear**

Opções de registro em log da VPN

Com os logs do Site-to-Site VPN, você pode obter acesso a detalhes sobre estabelecimento do túnel de segurança IP (IPsec), negociações do Internet Key Exchange (IKE) e mensagens de protocolo Dead Peer Detection (DPD).

Para ter mais informações, consulte [AWS Site-to-Site VPN troncos](#).

Formatos de log disponíveis: `json`, `text`

Versões do IKE

As versões do IKE que são permitidas para o túnel VPN. Você pode especificar um ou mais dos valores padrão.

Padrão: `ikev1`, `ikev2`

CIDR de IPv4 do túnel interno

O intervalo de endereços IPv4 internos para o túnel de VPN. É possível especificar um bloco CIDR de tamanho /30 a partir do intervalo `169.254.0.0/16`. O bloco CIDR deve ser exclusivo em todas as conexões Site-to-Site VPN que usam o mesmo gateway privado virtual.

Note

O bloco CIDR não precisa ser exclusivo em todas as conexões em um gateway de trânsito. No entanto, se eles não forem exclusivos, isso pode criar um conflito no gateway do cliente. Tenha cuidado ao reutilizar o mesmo bloco CIDR em várias conexões VPN Site-to-Site em um gateway de trânsito.

Os seguintes blocos CIDR são reservados e não podem ser usados:

- 169.254.0.0/30
- 169.254.1.0/30
- 169.254.2.0/30
- 169.254.3.0/30
- 169.254.4.0/30
- 169.254.5.0/30
- 169.254.169.252/30

Padrão: um bloco CIDR IPv4 de tamanho /30 do intervalo 169.254.0.0/16.

CIDR de IPv6 do túnel interno

(Somente conexões VPN IPv6) O intervalo de endereços IPv6 internos para o túnel de VPN. É possível especificar um bloco CIDR de tamanho /126 a partir do intervalo fd00::/8 local. O bloco CIDR deve ser exclusivo em todas as conexões Site-to-Site VPN que usam o mesmo gateway de trânsito.

Padrão: um bloco CIDR IPv6 de tamanho /126 do intervalo fd00::/8 local.

CIDR de rede IPv4 local

(Somente conexão VPN IPv4) O intervalo CIDR IPv4 no gateway do cliente (no local) que tem permissão para se comunicar pelos túneis de VPN.

Padrão: 0.0.0.0/0

CIDR de rede IPv4 remota

(Somente conexão VPN IPv4) O intervalo CIDR IPv4 no AWS lado que tem permissão para se comunicar pelos túneis VPN.

Padrão: 0.0.0.0/0

CIDR de rede IPv6 local

(Somente conexão VPN IPv6) O intervalo CIDR IPv6 no gateway do cliente (local) que tem permissão para se comunicar pelos túneis de VPN.

Padrão: ::/0

CIDR de rede IPv6 remota

(Somente conexão VPN IPv6) O intervalo CIDR IPv6 no AWS lado que tem permissão para se comunicar pelos túneis VPN.

Padrão: ::/0

Fase 1 Números de grupos Diffie-Hellman (DH)

Os números de grupos DH que são permitidos para o túnel VPN para a fase 1 das negociações de IKE. Você pode especificar um ou mais dos valores padrão.

Padrão: 2, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Fase 2 Números de grupos Diffie-Hellman (DH)

Os números de grupos DH que são permitidos para o túnel VPN para a fase 2 das negociações de IKE. Você pode especificar um ou mais dos valores padrão.

Padrão: 2, 5, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

Fase 1 Algoritmos de criptografia

Os algoritmos de criptografia permitidos para o túnel VPN para a fase 1 das negociações de IKE. Você pode especificar um ou mais dos valores padrão.

Padrão: AES128, AES256, AES128-GCM-16, AES256-GCM-16

Fase 2 Algoritmos de criptografia

Os algoritmos de criptografia permitidos para o túnel VPN para a fase 2 das negociações de IKE. Você pode especificar um ou mais dos valores padrão.

Padrão: AES128, AES256, AES128-GCM-16, AES256-GCM-16

Fase 1 Algoritmos de integridade

Os algoritmos de integridade permitidos para o túnel VPN para a fase 1 das negociações de IKE. Você pode especificar um ou mais dos valores padrão.

Padrão: SHA1, SHA2-256, SHA2-384, SHA2-512

Fase 2 Algoritmos de integridade

Os algoritmos de integridade permitidos para o túnel VPN para a fase 2 das negociações de IKE. Você pode especificar um ou mais dos valores padrão.

Padrão: SHA1, SHA2-256, SHA2-384, SHA2-512

Tempo de vida da fase 1

Note

AWS inicie as rechaves com os valores de tempo definidos nos campos Vida útil da Fase 1 e Vida útil da Fase 2. Se as vidas úteis forem diferentes dos valores negociados no handshake, isso poderá interromper a conectividade do túnel.

O tempo de vida em segundos da fase 1 da negociação de IKE. Você pode especificar um número entre 900 e 28.800.

Padrão: 28.800 (8 horas)

Tempo de vida da fase 2

Note

AWS inicie as rechaves com os valores de tempo definidos nos campos Vida útil da Fase 1 e Vida útil da Fase 2. Se as vidas úteis forem diferentes dos valores negociados no handshake, isso poderá interromper a conectividade do túnel.

O tempo de vida em segundos da fase 2 da negociação de IKE. Você pode especificar um número entre 900 e 3.600. O número especificado deve ser menor que o número de segundos para a vida útil da fase 1.

Padrão: 3.600 (1 hora)

Chaves pré-compartilhadas (PSK)

Chave pré-compartilhada (PSK) para estabelecer a associação de IKE (Internet key exchange – Troca de chaves da Internet) inicial entre o gateway de destino e o gateway do cliente.

O PSK deve estar entre 8 e 64 caracteres de extensão e não pode começar com zero (0). Os caracteres permitidos são alfanuméricos, pontos (.) e sublinhados (_).

Padrão: uma string de 32 caracteres alfanuméricos.

Fuzz de rechaveamento

A porcentagem da janela de rechaveamento (determinada pelo tempo de margem de rechaveamento) dentro da qual o tempo de rechaveamento é selecionado aleatoriamente.

Você pode especificar um valor percentual entre 0 e 100.

Padrão: 100

Tempo de margem de rechaveamento

O tempo de margem em segundos antes da expiração da vida útil das fases 1 e 2, durante o qual o AWS lado da conexão VPN executa uma rechave IKE.

Você pode especificar um número entre 60 e metade do valor de vida útil da fase 2.

A hora exata do rechaveamento é selecionada aleatoriamente com base no valor de fuzz de rechaveamento.

Padrão: 270 (4,5 minutos)

Reproduzir pacotes de tamanho da janela

O número de pacotes em uma janela de reprodução de IKE.

Você pode especificar um valor entre 64 e 2048.

Padrão: 1024

Ação de inicialização

A ação a ser realizada ao estabelecer o túnel para uma conexão VPN. Você pode especificar o seguinte:

- **Start:** AWS inicia a negociação do IKE para abrir o túnel. Somente compatível se o gateway do cliente estiver configurado com um endereço IP.
- **Add:** o dispositivo de gateway do cliente deve iniciar a negociação do protocolo IKE para ativar o túnel.

Para obter mais informações, consulte [Opções de iniciação de túnel do Site-to-Site VPN](#).

Padrão: Add

Controle de ciclo de vida do endpoint de túnel

O controle de ciclo de vida do endpoint de túnel oferece controle sobre o cronograma de substituições de endpoints.

Para ter mais informações, consulte [Controle de ciclo de vida do endpoint de túnel](#).

Padrão: Off

É possível especificar as opções de túnel ao criar uma conexão do Site-to-Site VPN ou modificar as opções de túnel para uma conexão VPN existente. Para obter mais informações, consulte os tópicos a seguir.

- [Etapa 5: criar uma conexão VPN](#)
- [Modificar opções de túnel do Site-to-Site VPN](#)

Opções de autenticação de túnel site a site VPN

Você pode usar chaves pré-compartilhadas ou certificados para autenticar seus endpoints de túnel site a site VPN.

Chaves pré-compartilhadas

Uma chave pré-compartilhada é a opção de autenticação padrão.

Uma chave pré-compartilhada é uma opção de VPN túnel site a site que você pode especificar ao criar um túnel site a site. VPN

Uma chave pré-compartilhada é uma string inserida ao configurar o dispositivo de gateway do cliente. Se você não especificar uma string, geraremos uma automaticamente para você. Para obter mais informações, consulte [O dispositivo de gateway do cliente](#).

Certificado privado de AWS Private Certificate Authority

Se você não quiser usar chaves pré-compartilhadas, você pode usar um certificado privado AWS Private Certificate Authority para autenticar suas. VPN

Crie um certificado privado de uma CA subordinada usando o AWS Private Certificate Authority (CA privada da AWS). Para assinar a CA ACM subordinada, você pode usar uma CA ACM raiz ou uma

CA externa. Para obter mais informações sobre como criar um certificado privado, consulte [Criar e gerenciar uma CA privada](#) no Guia do usuário do AWS Private Certificate Authority .

Você deve criar uma função vinculada ao serviço para gerar e usar o certificado para o AWS lado do endpoint do túnel site a siteVPN. Para obter mais informações, consulte [the section called “Funções vinculadas a serviço”](#).

Depois de gerar o certificado privado, especifique o certificado ao criar o gateway do cliente e aplicá-lo ao dispositivo de gateway do cliente.

Se você não especificar o endereço IP do dispositivo de gateway do cliente, não verificaremos o endereço IP. Essa operação permite mover o dispositivo de gateway do cliente para um endereço IP diferente sem precisar reconfigurar a VPN conexão.

O site a site VPN realiza a verificação da cadeia de certificados no certificado do gateway do cliente quando você cria um certificado. Além das verificações básicas de CA e validade, o Site-to-Site VPN verifica se as extensões X.509 estão presentes, incluindo Identificador de Chave de Autoridade, Identificador de Chave de Assunto e Restrições Básicas.

Opções de iniciação de túnel do Site-to-Site VPN

Por padrão, o dispositivo de gateway do cliente deve ativar os túneis para a conexão do Site-to-Site VPN gerando tráfego e iniciando o processo de negociação do protocolo IKE. Você pode configurar seus túneis VPN para especificar que, em vez disso, AWS devem iniciar ou reiniciar o processo de negociação do IKE.

Opções de iniciação do protocolo IKE de túnel da VPN

As seguintes opções de iniciação do protocolo IKE estão disponíveis. Você pode implementar uma ou ambas as opções para um ou ambos os túneis da conexão do Site-to-Site VPN. Consulte [Opções de túnel VPN](#) para obter mais detalhes sobre essas e outras configurações de opções de túnel.

- **Ação de inicialização:** a ação a ser executada ao estabelecer o túnel da VPN para uma conexão VPN nova ou modificada. Por padrão, o dispositivo de gateway do cliente inicia o processo de negociação do protocolo IKE para ativar o túnel. Você pode especificar que, em vez disso, AWS deve iniciar o processo de negociação do IKE.
- **Ação de tempo limite do DPD:** a ação a ser executada após atingir o tempo limite do Dead Peer Detection (DPD). Por padrão, a sessão do protocolo IKE é interrompida, o túnel fica inativo e as

rotas são removidas. Você pode especificar que AWS deve reiniciar a sessão IKE quando ocorrer o tempo limite do DPD, ou você pode especificar que não AWS deve realizar nenhuma ação quando o tempo limite do DPD ocorrer.

Regras e limitações

As seguintes regras e limitações são aplicáveis:

- Para iniciar a negociação do IKE, é AWS necessário o endereço IP público do seu dispositivo de gateway do cliente. Se você configurou a autenticação baseada em certificado para sua conexão VPN e não especificou um endereço IP ao criar o recurso de gateway do cliente AWS, deverá criar um novo gateway do cliente e especificar o endereço IP. Depois, modifique a conexão VPN e especifique o novo gateway do cliente. Para ter mais informações, consulte [Alterar o gateway do cliente para uma conexão do Site-to-Site VPN](#).
- A iniciação IKE (ação de inicialização) do AWS lado da conexão VPN é suportada somente para IKEv2.
- Se estiver usando a iniciação IKE do AWS lado da conexão VPN, ela não inclui uma configuração de tempo limite. Ela tentará continuamente estabelecer uma conexão até conseguir. Além disso, o AWS lado da conexão VPN reiniciará a negociação do IKE ao receber uma mensagem SA de exclusão do gateway do cliente.
- Se o dispositivo de gateway do cliente estiver atrás de um firewall ou de outro dispositivo usando a Conversão de endereços de rede (NAT), ele deverá ter uma identidade (IDr) configurada. Para obter mais informações sobre o IDr, consulte [RFC 7296](#).

Se você não configurar a iniciação do IKE pela AWS lateral do túnel VPN e a conexão VPN passar por um período de inatividade (geralmente 10 segundos, dependendo da configuração), o túnel poderá cair. Para evitar isso, você pode usar uma ferramenta de monitoramento de rede que envie pings keepalive.

Trabalhar com opções de iniciação de túnel da VPN

Para obter mais informações sobre como trabalhar com opções de iniciação de túnel da VPN, consulte os seguintes tópicos:

- Para criar uma conexão VPN e especificar as opções de iniciação de túnel da VPN: [Etapa 5: criar uma conexão VPN](#)

- Para modificar as opções de iniciação de túnel da VPN em uma conexão VPN existente: [Modificar opções de túnel do Site-to-Site VPN](#)

Substituições de endpoint de túnel Site-to-Site VPN

Sua conexão do Site-to-Site VPN consiste em dois túneis da VPN para redundância. Às vezes, um ou ambos os endpoints do túnel VPN são substituídos ao AWS realizar atualizações do túnel ou quando você modifica sua conexão VPN. Durante a substituição de um endpoint de túnel, a conectividade através do túnel pode ser interrompida enquanto o novo endpoint de túnel é provisionado.

Tópicos

- [Substituições de endpoint iniciadas pelo cliente](#)
- [Substituições de endpoints gerenciados pela AWS](#)
- [Controle de ciclo de vida do endpoint de túnel](#)

Substituições de endpoint iniciadas pelo cliente

Quando você modifica os seguintes componentes de sua conexão VPN, um ou ambos os endpoints do túnel são substituídos.

Modificação	Ação API	Impacto do túnel
Modificar o gateway de destino para a conexão VPN	ModifyVpnConnection	Ambos os túneis estão indisponíveis enquanto novos endpoints do túnel são provisionados.
Alterar o gateway do cliente para a conexão VPN	ModifyVpnConnection	Ambos os túneis estão indisponíveis enquanto novos endpoints do túnel são provisionados.
Modificar as opções da conexão VPN	ModifyVpnConnectionOptions	Ambos os túneis estão indisponíveis enquanto

Modificação	Ação API	Impacto do túnel
		novos endpoints do túnel são provisionados.
Modificar as opções do túnel da VPN	ModifyVpnTunnelOptions	O túnel modificado não está disponível durante a atualização.

Substituições de endpoints gerenciados pela AWS

AWS Site-to-Site VPN é um serviço gerenciado e aplica periodicamente atualizações aos endpoints do túnel VPN. Essas atualizações acontecem por vários motivos, incluindo os seguintes:

- Como aplicar atualizações gerais, como patches, aprimoramentos de resiliência e outras melhorias
- Para retirar o hardware subjacente
- Quando o monitoramento automatizado determina que um endpoint de túnel da VPN não está íntegro

AWS aplica atualizações de endpoint de túnel a um túnel de sua conexão VPN por vez. Durante uma atualização de endpoint de túnel, sua conexão de VPN pode sofrer uma breve perda de redundância. Portanto, é importante configurar ambos os túneis em sua conexão VPN para alta disponibilidade.

Controle de ciclo de vida do endpoint de túnel

O controle do ciclo de vida do endpoint do túnel fornece controle sobre o cronograma de substituições do endpoint e pode ajudar a minimizar as interrupções de conectividade durante as substituições gerenciadas do endpoint do túnel. AWS Com esse recurso, você pode optar por aceitar atualizações AWS gerenciadas para endpoints de túnel no momento que for melhor para sua empresa. Utilize esse recurso se você tiver necessidades comerciais de curto prazo ou só puder comportar um túnel por conexão de VPN.

Note

Em raras circunstâncias, AWS pode aplicar atualizações críticas aos endpoints do túnel imediatamente, mesmo se o recurso de controle do ciclo de vida do endpoint do túnel estiver ativado.

Tópicos

- [Como o controle de ciclo de vida do endpoint de túnel funciona](#)
- [Habilitar o controle de ciclo de vida do endpoint de túnel](#)
- [Verificar se o controle de ciclo de vida do endpoint de túnel está habilitado](#)
- [Verificar se há atualizações disponíveis](#)
- [Aceitar uma atualização de manutenção](#)
- [Desativar o controle de ciclo de vida do endpoint de túnel](#)

Como o controle de ciclo de vida do endpoint de túnel funciona

Ative o recurso de controle de ciclo de vida do endpoint de túnel para túneis individuais em uma conexão de VPN. Ele pode ser habilitado no momento da criação da VPN ou modificando as opções de túnel para uma conexão de VPN existente.

Depois que o controle de ciclo de vida do endpoint de túnel for habilitado, você obterá visibilidade adicional sobre os próximos eventos de manutenção do túnel de duas maneiras:

- Você receberá AWS Health notificações sobre futuras substituições de terminais de túneis.
- [O status da manutenção pendente, junto com os carimbos de data/hora da Manutenção aplicada automaticamente após e da Última manutenção aplicada, pode ser visto no AWS Management Console ou usando o `get-vpn-tunnel-replacement` comando `-status`. AWS CLI](#)

Quando a manutenção de um endpoint de túnel estiver disponível, você terá a oportunidade de aceitar a atualização em um horário que seja conveniente para você, antes do determinado carimbo de data e hora Manutenção aplicada automaticamente após.

Se você não aplicar as atualizações antes da data de aplicação automática da Manutenção, AWS executará automaticamente a substituição do endpoint do túnel logo depois, como parte do ciclo regular de atualização de manutenção.

Habilitar o controle de ciclo de vida do endpoint de túnel

Você pode ativar esse recurso usando o AWS Management Console ou AWS CLI.

Note

Por padrão, quando o recurso para uma conexão de VPN existente é ativado, uma substituição de endpoints de túnel é iniciada ao mesmo tempo. Se quiser ativar o recurso, mas não iniciar a substituição imediata do endpoint de túnel, você pode utilizar a opção Ignorar substituição do túnel.

Existing VPN connection

As etapas a seguir demonstram como habilitar o controle de ciclo de vida do endpoint de túnel em uma conexão de VPN existente.

Como habilitar o controle de ciclo de vida do endpoint de túnel utilizando a AWS Management Console

1. Abra o console do Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação esquerdo, selecione Conexões Site-to-Site VPN.
3. Selecione a conexão apropriada em Conexões de VPN.
4. Selecione Ações, Modificar opções de túnel de VPN.
5. Selecione o túnel específico que você deseja modificar escolhendo o Endereço IP externo do túnel VPN apropriado.
6. Em Controle de ciclo de vida do endpoint de túnel, marque a caixa de seleção Habilitar.
7. (Opcional) Selecione Ignorar substituição de túnel.
8. Escolha Salvar alterações.

Como habilitar o controle de ciclo de vida do endpoint de túnel utilizando a AWS CLI

Use o [modify-vpn-tunnel-options](#) comando para ativar o controle do ciclo de vida do endpoint do túnel.

New VPN connection

As etapas a seguir demonstram como habilitar o controle de ciclo de vida do endpoint de túnel durante a criação de uma conexão de VPN.

Para habilitar o controle do ciclo de vida do endpoint do túnel durante a criação de uma nova conexão VPN usando o AWS Management Console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões de VPN de local a local.
3. Escolha Create VPN Connection (Criar conexão VPN).
4. Nas seções de Opções de túnel 1 e Opções de túnel 2, em Controle de ciclo de vida do endpoint de túnel, selecione Habilitar.
5. Escolha Create VPN Connection (Criar conexão VPN).

Para habilitar o controle do ciclo de vida do endpoint do túnel durante a criação de uma nova conexão VPN usando o AWS CLI

Use o [create-vpn-connection](#) comando para ativar o controle do ciclo de vida do endpoint do túnel.

Verificar se o controle de ciclo de vida do endpoint de túnel está habilitado

Você pode verificar se o controle do ciclo de vida do endpoint do túnel está habilitado em um túnel VPN existente usando a CLI ou AWS Management Console .

Como verificar se o controle de ciclo de vida do endpoint de túnel está habilitado utilizando o AWS Management Console

1. Abra o console do Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação esquerdo, selecione Conexões Site-to-Site VPN.
3. Selecione a conexão apropriada em Conexões de VPN.
4. Selecione a guia Detalhes do túnel.
5. Nos detalhes do túnel, procure Controle de ciclo de vida do endpoint de túnel, que informará se o recurso está habilitado ou desabilitado.

Como verificar se o controle de ciclo de vida do endpoint de túnel está habilitado utilizando o AWS CLI

Use o [describe-vpn-connections](#) comando para verificar se o controle do ciclo de vida do endpoint do túnel está ativado.

Verificar se há atualizações disponíveis

Depois de habilitar o recurso de controle de ciclo de vida do endpoint de túnel, você pode visualizar se uma atualização de manutenção está disponível para sua conexão de VPN utilizando o AWS Management Console ou a CLI.

Para verificar as atualizações disponíveis usando o AWS Management Console

1. Abra o console do Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação esquerdo, selecione Conexões Site-to-Site VPN.
3. Selecione a conexão apropriada em Conexões de VPN.
4. Selecione a guia Detalhes do túnel.
5. Confira a coluna Manutenção pendente. O status será Disponível ou Nenhum.

Para verificar as atualizações disponíveis usando o AWS CLI

Use o comando [get-vpn-tunnel-replacement-status](#) para verificar as atualizações disponíveis.

Aceitar uma atualização de manutenção

Quando uma atualização de manutenção está disponível, você pode aceitá-la usando a CLI AWS Management Console ou.

Para aceitar uma atualização de manutenção disponível usando o AWS Management Console

1. Abra o console do Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação esquerdo, selecione Conexões Site-to-Site VPN.
3. Selecione a conexão apropriada em Conexões de VPN.
4. Selecione Ações e, depois, Substituir túnel VPN.
5. Selecione o túnel específico que você deseja substituir escolhendo o Endereço IP externo do túnel VPN.
6. Selecione Replace (Substituir).

Para aceitar uma atualização de manutenção disponível usando o AWS CLI

Use o [replace-vpn-tunnel](#) comando para aceitar uma atualização de manutenção disponível.

Desativar o controle de ciclo de vida do endpoint de túnel

Se você não quiser mais usar o recurso de controle do ciclo de vida do endpoint de túnel, poderá desativá-lo usando o AWS Management Console ou o AWS CLI. Quando você desativar esse recurso, a AWS implantará as atualizações de manutenção automaticamente e periodicamente, e elas poderão ocorrer durante o horário comercial. Para evitar qualquer impacto, é altamente recomendável configurar os dois túneis em sua conexão de VPN para alta disponibilidade.

Note

Embora haja uma manutenção pendente disponível, você não pode especificar a opção Ignorar substituição de túnel ao desativar o recurso. Você sempre pode desativar o recurso sem usar a opção ignorar a substituição do túnel, mas AWS implantará automaticamente as atualizações de manutenção pendentes disponíveis iniciando imediatamente a substituição do endpoint do túnel.

Para desativar o controle do ciclo de vida do endpoint do túnel usando o AWS Management Console

1. Abra o console do Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação esquerdo, selecione Conexões Site-to-Site VPN.
3. Selecione a conexão apropriada em Conexões de VPN.
4. Selecione Ações, Modificar opções de túnel de VPN.
5. Selecione o túnel específico que você deseja modificar escolhendo o Endereço IP externo do túnel VPN apropriado.
6. Para desativar o controle de ciclo de vida do endpoint de túnel, em Controle de ciclo de vida do endpoint de túnel, desmarque a caixa de seleção Habilitar.
7. (Opcional) Selecione Ignorar substituição de túnel.
8. Escolha Salvar alterações.

Para desativar o controle do ciclo de vida do endpoint do túnel usando o AWS CLI

Use o [modify-vpn-tunnel-options](#) comando para desativar o controle do ciclo de vida do endpoint do túnel.

Opções de gateway do cliente para a conexão de VPN de local a local

A tabela a seguir descreve as informações necessárias para criar um recurso de gateway do cliente na AWS.

Item	Descrição
(Opcional) Etiqueta de nome.	Cria uma etiqueta com a chave de “Nome” e um valor especificado por você.
(Apenas roteamento dinâmico) Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) do gateway do cliente.	<p>Há suporte para ASN na faixa de 1 a 4.294.967.295. É possível usar um ASN público já existente e atribuído para a rede, com exceção do seguinte:</p> <ul style="list-style-type: none"> • 7224: reservado em todas as Regiões • 9059: reservado na região eu-west-1 • 10124: reservado na região ap-northeast-1 • 17943: reservado na região ap-southeast-1 <p>Se você não tiver um ASN público, poderá usar um ASN privado na faixa de 64.512 a 65.534 ou 4.200.000.000 a 4.294.967.294. O ASN padrão é 65000. Consulte Opções de roteamento site a VPN site para obter mais detalhes sobre o roteamento.</p>
(Opcional) O endereço IP da interface externa do dispositivo do gateway do cliente.	<p>O endereço IP deve ser estático.</p> <p>Se o dispositivo de gateway do cliente estiver atrás de um dispositivo de conversão de endereços de rede (NAT), use o endereço IP do dispositivo NAT. Além disso, certifique-se de</p>

Item	Descrição
	<p>que os pacotes UDP na porta 500 (e na porta 4500, se o NAT-Traversal estiver sendo usado) possam passar entre sua rede e os endpoints . AWS Site-to-Site VPN Consulte Regras de firewall para obter mais informações.</p> <p>Não é necessário um endereço IP quando você está usando um certificado privado AWS Private Certificate Authority e uma VPN pública.</p>

Item	Descrição
<p>(Opcional) Certificado privado de uma CA subordinada usando AWS Certificate Manager (ACM).</p>	<p>Se você quiser usar a autenticação baseada em certificado, forneça o ARN de um certificado privado do ACM que será usado no dispositivo de gateway do cliente.</p> <p>Ao criar um gateway do cliente, você pode configurá-lo para usar certificados privados do AWS Private Certificate Authority para autenticar a VPN de local a local.</p> <p>Ao optar por usar essa opção, você cria uma autoridade AWS de certificação (CA) privada totalmente hospedada para uso interno da sua organização. Tanto o certificado de CA raiz quanto os certificados de CA subordinados são armazenados e gerenciados pelo CA privada da AWS.</p> <p>Antes de criar o gateway do cliente, você cria um certificado privado de uma CA subordinada usando e AWS Private Certificate Authority, em seguida, especifica o certificado ao configurar o gateway do cliente. Para obter informações sobre como criar um certificado privado, consulte Criar e gerenciar uma CA privada no Guia do usuário do AWS Private Certificate Authority .</p>
<p>(Opcional) Dispositivo.</p>	<p>Um nome para o dispositivo de gateway do cliente associado a esse gateway do cliente.</p>

Conexões Site-to-Site VPN aceleradas

Opcionalmente, você pode habilitar a aceleração para sua conexão do Site-to-Site VPN. Uma conexão VPN acelerada Site-to-Site (conexão VPN acelerada AWS Global Accelerator) é usada

para rotear o tráfego da sua rede local para um ponto de presença mais próximo do dispositivo AWS de gateway do cliente. AWS Global Accelerator otimiza o caminho da rede, usando a rede AWS global livre de congestionamento para rotear o tráfego para o endpoint que fornece o melhor desempenho do aplicativo (para obter mais informações, consulte). [AWS Global Accelerator](#) Você pode usar uma conexão VPN acelerada para evitar interrupções de rede que possam ocorrer quando o tráfego é roteado pela Internet pública.

Quando você cria uma conexão VPN acelerada, criamos e gerenciamos dois aceleradores em seu nome, um para cada túnel VPN. Você não pode visualizar ou gerenciar esses aceleradores sozinho usando o AWS Global Accelerator console ou as APIs.

Para obter informações sobre as AWS regiões que oferecem suporte a conexões VPN aceleradas, consulte as perguntas frequentes sobre [VPN AWS acelerada de site a site](#).

Habilitar a aceleração

Por padrão, quando você cria uma conexão do Site-to-Site VPN, a aceleração é desabilitada. Opcionalmente, você pode habilitar a aceleração ao criar um anexo do Site-to-Site VPN em um gateway de trânsito. Para obter mais informações e etapas, consulte [Criar um anexo de VPN do gateway de trânsito](#).

As conexões VPN aceleradas usam um grupo separado de endereços IP para os endereços IP do endpoint do túnel. Os endereços IP dos dois túneis VPN são selecionados em duas [zonas de rede](#) separadas.

Regras e restrições

Para usar uma conexão VPN acelerada, aplicam-se as seguintes regras:

- A aceleração só é compatível com conexões do Site-to-Site VPN anexadas a um gateway de trânsito. Os gateways privados virtuais não são compatíveis com conexões VPN aceleradas.
- Uma conexão VPN acelerada de site a site não pode ser usada com uma interface virtual pública. AWS Direct Connect
- Não é possível habilitar ou desabilitar a aceleração de uma conexão do Site-to-Site VPN existente. Em vez disso, você pode criar uma conexão do Site-to-Site VPN com a aceleração habilitada ou desabilitada conforme necessário. Configure seu dispositivo de gateway do cliente para usar a nova conexão do Site-to-Site VPN e exclua a conexão do Site-to-Site VPN antiga.

- O NAT-traversal (NAT-T) é necessário para uma conexão VPN acelerada e é habilitado por padrão. Se você fez download de um [arquivo de configuração](#) do console da Amazon VPC, verifique a configuração NAT-T e ajuste-a, se necessário.
- A negociação IKE para túneis VPN acelerados deve ser iniciada a partir do dispositivo de gateway do cliente. As duas opções de túnel que afetam esse comportamento são `Startup Action DPD Timeout Action` e. Consulte [Opções de túnel VPN](#) e [Opções de iniciação do túnel da VPN](#) para obter mais informações.
- As conexões VPN site-to-site que usam autenticação baseada em certificado podem não ser compatíveis AWS Global Accelerator com, devido ao suporte limitado à fragmentação de pacotes no Global Accelerator. Para obter mais informações, consulte [Como o AWS Global Accelerator funciona](#). Se for necessária uma conexão VPN acelerada que use a autenticação baseada em certificado, o dispositivo de gateway do cliente deverá oferecer suporte à fragmentação IKE. Caso contrário, não habilite sua VPN para aceleração.

Opções de roteamento site a VPN site

AWS recomenda anunciar BGP rotas específicas para influenciar as decisões de roteamento no gateway privado virtual. Verifique as informações sobre comandos específicos do dispositivo na documentação do fornecedor.

Quando você cria várias VPN conexões, o gateway privado virtual envia tráfego de rede para a VPN conexão apropriada usando rotas atribuídas estaticamente ou BGP anúncios de rotas. A rota depende de como a VPN conexão foi configurada. As rotas atribuídas estaticamente são preferidas às rotas BGP anunciadas nos casos em que existem rotas idênticas no gateway privado virtual. Se você selecionar a opção de usar BGP publicidade, não poderá especificar rotas estáticas.

Para obter mais informações sobre prioridade de rotas, consulte [Tabelas de rotas e prioridade de VPN rotas](#).

Ao criar uma VPN conexão site a site, você deve fazer o seguinte:

- Especifique o tipo de roteamento que você planeja usar (estático ou dinâmico)
- Atualize a [tabela de rotas](#) da sub-rede

Existem cotas para o número de rotas que podem ser adicionadas a uma tabela de rotas. Para obter mais informações, consulte a seção Tabelas de rotas nas [VPCcotas da Amazon](#) no Guia do VPC usuário da Amazon.

Tópicos

- [Roteamento estático e dinâmico](#)
- [Tabelas de rotas e prioridade de VPN rotas](#)
- [Roteamento durante atualizações do endpoint VPN do túnel](#)
- [Tráfego IPv4 e IPv6](#)

Roteamento estático e dinâmico

O tipo de roteamento selecionado pode depender da marca e do modelo do dispositivo de gateway do cliente. Se o dispositivo de gateway do cliente suportar o Border Gateway Protocol (BGP), especifique o roteamento dinâmico ao configurar sua conexão site a siteVPN. Se o dispositivo de gateway do cliente não suportarBGP, especifique o roteamento estático.

Se você usa um dispositivo compatível com BGP publicidade, não especifica rotas estáticas para a VPN conexão site a site porque o dispositivo usa BGP para anunciar suas rotas para o gateway privado virtual. Se você usa um dispositivo que não suporta BGP publicidade, deve selecionar o roteamento estático e inserir as rotas (prefixos IP) da sua rede que devem ser comunicadas ao gateway privado virtual.

Recomendamos que você use dispositivos BGP compatíveis, quando disponíveis, porque o BGP protocolo oferece verificações robustas de detecção de atividade que podem ajudar no failover para o segundo VPN túnel se o primeiro túnel cair. Dispositivos que não oferecem suporte também BGP podem realizar verificações de saúde para auxiliar no failover para o segundo túnel, quando necessário.

Você deve configurar seu dispositivo de gateway do cliente para rotear o tráfego da sua rede local para a conexão site a siteVPN. A configuração depende da marca e do modelo do seu dispositivo. Para obter mais informações, consulte [O dispositivo de gateway do cliente](#).

Tabelas de rotas e prioridade de VPN rotas

[As tabelas de rotas](#) determinam para onde o seu tráfego de rede VPC é direcionado. Em sua tabela de VPC rotas, você deve adicionar uma rota para sua rede remota e especificar o gateway privado virtual como destino. Isso permite VPC que o tráfego de sua rede remota, destinado à sua rede remota, seja roteado pelo gateway privado virtual e por um dos VPN túneis. Você pode habilitar a propagação automática de rotas da rede para a tabela de rotas.

Para determinar como o tráfego deve ser roteado, usamos a rota mais específica em sua tabela de rotas que corresponde ao tráfego (correspondência de prefixo mais longa). Se a tabela de rotas tiver rotas sobrepostas ou correspondentes, as seguintes regras serão aplicadas:

- Se as rotas propagadas de uma conexão site a site ou AWS Direct Connect a VPN conexão se sobrepuserem à rota local da sua VPC, a rota local será a preferida, mesmo que as rotas propagadas sejam mais específicas.
- Se as rotas propagadas de uma VPN conexão ou AWS Direct Connect conexão site a site tiverem o mesmo CIDR bloco de destino de outras rotas estáticas existentes (a correspondência de prefixo mais longa não pode ser aplicada), priorizamos as rotas estáticas cujos destinos são um gateway de internet, um gateway privado virtual, uma interface de rede, uma ID de instância, uma conexão de VPC peering, um gateway, um gateway de trânsito ou um endpoint de NAT gateway. VPC

Por exemplo, a tabela de rotas a seguir tem uma rota estática para um gateway da Internet e uma rota propagada para um gateway privado virtual. O destino de ambas as rotas é 172.31.0.0/24. Nesse caso, todo tráfego destinado para 172.31.0.0/24 é roteado para o gateway da Internet – é uma rota estática e, portanto, tem prioridade sobre a rota propagada.

Destino	Destino
10.0.0.0/16	Local
172.31.0.0/24	vgw-11223344556677889 (propagado)
172.31.0.0/24	igw-12345678901234567 (estático)

Somente prefixos IP conhecidos pelo gateway privado virtual, seja por meio de BGP anúncios ou de uma entrada de rota estática, podem receber tráfego do seu VPC. O gateway privado virtual não roteia nenhum outro tráfego destinado fora dos BGP anúncios recebidos, das entradas de rotas estáticas ou de seus anexos. VPC CIDR Os gateways privados virtuais não oferecem suporte ao IPv6 tráfego.

Quando um gateway privado virtual recebe informações de roteamento, ele usa a seleção de caminho para determinar como rotear o tráfego. A correspondência de prefixo mais longa se aplicará se todos os endpoints estiverem íntegros. A integridade de um endpoint de túnel tem precedência sobre outros atributos de roteamento. Essa precedência se aplica a VPNs gateways privados virtuais

e gateways de trânsito. Se os prefixos forem os mesmos, o gateway privado virtual prioriza as rotas da seguinte forma, da mais preferida para a menos preferida:

- BGP rotas propagadas de uma conexão AWS Direct Connect
- Rotas estáticas adicionadas manualmente para uma conexão site VPN a site
- BGP rotas propagadas de uma conexão site a site VPN
- Para combinar prefixos usados por cada VPN conexão site a site BGP, o AS PATH é comparado e o prefixo com o AS mais curto é preferido. PATH

Note

AWS recomenda fortemente o uso de dispositivos de gateway do cliente que suportem roteamento assimétrico.

Para dispositivos de gateway de clientes que suportam roteamento assimétrico, não recomendamos o uso de AS PATH preendente, para garantir que ambos os túneis tenham AS igual. PATH Isso ajuda a garantir que o valor multi-exit discriminator (MED) que definimos em um túnel durante as [atualizações do endpoint VPN do túnel](#) seja usado para determinar a prioridade do túnel.

Para dispositivos de gateway do cliente que não oferecem suporte ao roteamento assimétrico, você pode usar o AS PATH preendente e o Local Preference para preferir um túnel ao outro. No entanto, quando o caminho de saída muda, o tráfego pode cair.

- Quando o PATHs AS tem o mesmo comprimento e se o primeiro AS no AS_SEQUENCE é o mesmo em vários caminhos, multi-exit discriminators (MEDs) são comparados. O caminho com o MED valor mais baixo é o preferido.

A prioridade da rota é afetada durante as [atualizações VPN do endpoint do túnel](#).

Em uma VPN conexão site a site, AWS seleciona um dos dois túneis redundantes como o caminho de saída principal. Essa seleção pode mudar às vezes, e é altamente recomendável que você configure ambos os túneis para alta disponibilidade e permita o roteamento assimétrico. A integridade de um endpoint de túnel tem precedência sobre outros atributos de roteamento. Essa precedência se aplica a VPNs gateways privados virtuais e gateways de trânsito.

Para um gateway privado virtual, um túnel em todas as VPN conexões site a site no gateway será selecionado. Para usar mais de um túnel, recomendamos explorar o Equal Cost Multipath (ECMP), que é compatível com VPN conexões site a site em um gateway de trânsito. Para obter

mais informações, consulte [Gateways de trânsito](#) no Amazon VPC Transit Gateways. ECMP não é compatível com VPN conexões site a site em um gateway privado virtual.

Para VPN conexões site a site que usam BGP, o túnel primário pode ser identificado pelo valor multi-exit discriminator (MED). Recomendamos anunciar BGP rotas mais específicas para influenciar as decisões de roteamento.

Para VPN conexões site a site que usam roteamento estático, o túnel principal pode ser identificado por estatísticas ou métricas de tráfego.

Roteamento durante atualizações do endpoint VPN do túnel

Uma VPN conexão site a site consiste em dois VPN túneis entre um dispositivo de gateway do cliente e um gateway privado virtual ou um gateway de trânsito. Recomendamos que você configure ambos os túneis para redundância. De tempos em tempos, AWS também realiza manutenção de rotina em sua VPN conexão, o que pode desativar brevemente um dos dois túneis de sua VPN conexão. Para obter mais informações, consulte [Notificações de substituição de endpoint do túnel](#).

Quando realizamos atualizações em um VPN túnel, definimos um valor menor de outbound multi-exit discriminator (MED) no outro túnel. Se você configurou seu dispositivo de gateway do cliente para usar os dois túneis, sua VPN conexão usa o outro túnel (ascendente) durante o processo de atualização do endpoint do túnel.

Note

Para garantir que o túnel ascendente com o inferior MED seja preferido, certifique-se de que seu dispositivo de gateway do cliente use os mesmos valores de peso e preferência local para ambos os túneis (peso e preferência local têm maior prioridade do que MED).

Tráfego IPv4 e IPv6

A conexão do Site-to-Site VPN em um gateway de trânsito pode ser compatível com tráfego IPv4 ou IPv6 dentro dos túneis VPN. Por padrão, uma conexão do Site-to-Site VPN é compatível com o tráfego IPv4 dentro dos túneis VPN. É possível configurar uma nova conexão do Site-to-Site VPN para ser compatível com o tráfego IPv6 dentro dos túneis VPN. Depois, se a VPC e a rede local estiverem configuradas para endereçamento IPv6, você poderá enviar tráfego IPv6 pela conexão VPN.

Se você habilitar o IPv6 para os túneis VPN da conexão do Site-to-Site VPN, cada túnel terá dois blocos CIDR. Um é um bloco CIDR do IPv4 de tamanho /30 e o outro é um bloco CIDR do IPv6 de tamanho /126.

As seguintes regras se aplicam:

- Endereços IPv6 são compatíveis apenas com os endereços IP internos dos túneis VPN. Os endereços IP do túnel externo para os AWS endpoints são endereços IPv4, e o endereço IP público do gateway do cliente deve ser um endereço IPv4.
- As conexões do Site-to-Site VPN em um gateway privado virtual não são compatíveis com IPv6.
- Não é possível habilitar o suporte a IPv6 para uma conexão existente do Site-to-Site VPN.
- Uma conexão do Site-to-Site VPN não é compatível com tráfego IPv4 e IPv6.

Para obter mais informações sobre como criar uma conexão VPN, consulte [Etapa 5: criar uma conexão VPN](#).

Começando com AWS Site-to-Site VPN

Use o procedimento a seguir para configurar uma AWS Site-to-Site VPN conexão. Durante a criação, especifique um gateway privado virtual, um gateway de trânsito ou “Não associado” como o tipo de gateway de destino. Se você especificar “Não associado”, poderá escolher o tipo de gateway de destino posteriormente ou usá-lo como um anexo VPN para o AWS Cloud WAN. Este tutorial ajuda você a criar uma conexão VPN usando um gateway privado virtual. Ele presume que você já tenha uma VPC com uma ou mais sub-redes.

Para configurar uma conexão VPN usando um gateway privado virtual, conclua as seguintes etapas:

Tarefas

- [Pré-requisitos](#)
- [Etapa 1: criar um gateway do cliente](#)
- [Etapa 2: criar um gateway de destino](#)
- [Etapa 3: configurar o roteamento](#)
- [Etapa 4: atualizar o grupo de segurança](#)
- [Etapa 5: criar uma conexão VPN](#)
- [Etapa 6: baixar o arquivo de configuração](#)
- [Etapa 7: configurar o dispositivo de gateway do cliente](#)

Tarefas relacionadas

- Para criar uma conexão VPN para o AWS Cloud WAN, consulte [Crie um anexo VPN para AWS Cloud WAN](#).
- Para criar uma conexão VPN em um gateway de trânsito, consulte [Criar um anexo de VPN do gateway de trânsito](#).

Pré-requisitos

Você precisa das informações a seguir para definir e configurar os componentes de uma conexão VPN.

Item	Informações
Dispositivo de gateway do cliente	<p>O dispositivo físico ou de software no seu lado da conexão VPN. Você precisa do fornecedor (por exemplo, Cisco), da plataforma (por exemplo, roteadores da série ISR) e da versão do software (por exemplo, IOS 12.4).</p>
Gateway do cliente	<p>Para criar o recurso de gateway do cliente em AWS, você precisa das seguintes informações:</p> <ul style="list-style-type: none">• O endereço IP roteável na Internet para a interface externa do dispositivo.• O tipo de roteamento: estático ou dinâmico• Para roteamento dinâmico, o número de sistema autônomo (ASN) do Border Gateway Protocol (BGP)• (Opcional) Certificado privado de AWS Private Certificate Authority para autenticar sua VPN <p>Para ter mais informações, consulte Opções de gateway do cliente.</p>
(Opcional) O ASN para o AWS lado da sessão do BGP	<p>Isso é especificado ao criar um gateway privado virtual ou um gateway de trânsito. Se você não especificar um valor, o ASN padrão será aplicado. Para obter mais informações, consulte Gateway privado virtual.</p>
Conexão VPN	<p>Para criar uma conexão VPN, você precisa das seguintes informações:</p> <ul style="list-style-type: none">• Para roteamento estático, os prefixos IP para a rede privada.• (Opcional) Opções de túnel para cada túnel de VPN. Para ter mais informações, consulte

Item	Informações
	Opções de túnel para a conexão do Site-to-Site VPN.

Etapa 1: criar um gateway do cliente

Um gateway do cliente fornece informações AWS sobre seu dispositivo de gateway do cliente ou aplicativo de software. Para ter mais informações, consulte [Gateway do cliente](#).

Se você planeja usar um certificado privado para autenticar sua VPN, crie um certificado privado de uma CA subordinada usando AWS Private Certificate Authority. Para obter informações sobre como criar um certificado privado, consulte [Criar e gerenciar uma CA privada](#) no Guia do usuário do AWS Private Certificate Authority .

Note

É necessário especificar um endereço IP ou o nome de recurso da Amazon do certificado privado.

Para criar um gateway do cliente usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Gateways do cliente.
3. Escolha Criar gateway do cliente.
4. (Opcional) Em Name (Nome), insira um nome para o gateway do cliente. Ao fazer isso, é criada uma tag com a chave Name e o valor especificado.
5. Para BGP ASN, informe o Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) do gateway do cliente.
6. (Opcional) Em IP address (Endereço IP), insira o endereço IP estático roteável pela Internet do dispositivo de gateway do cliente. Se o dispositivo de gateway do cliente estiver atrás de um dispositivo NAT que seja habilitado para NAT-T, use o endereço IP público do dispositivo NAT.
7. (Opcional) Se você quiser usar um certificado privado, em Certificate ARN (Certificado ARN), selecione o nome de recurso da Amazon do certificado privado.

8. (Opcional) Em Dispositivo, insira um nome para o gateway do cliente associado a esse gateway do cliente.
9. Escolha Criar gateway do cliente.

Para criar um gateway do cliente usando a linha de comando ou a API

- [CreateCustomerGateway](#)(API de consulta do Amazon EC2)
- [create-customer-gateway](#) (AWS CLI)
- [New-EC2CustomerGateway](#) (AWS Tools for Windows PowerShell)

Etapa 2: criar um gateway de destino

Para estabelecer uma conexão VPN entre sua VPC e sua rede local, você deve criar um gateway de destino no AWS lado da conexão. O gateway de destino pode ser um gateway privado virtual ou um gateway de trânsito.

Criar um gateway privado virtual

Quando você cria um gateway privado virtual, é possível especificar um Número de sistema autônomo (ASN) privado e personalizado para o lado da Amazon do gateway ou usar o ASN padrão da Amazon. Esse ASN deve ser diferente do BGP ASN especificado para o gateway do cliente.

Depois que você criar um gateway privado virtual, você deve anexá-lo à sua VPC.

Para criar um gateway privado virtual e anexá-lo à sua VPC

1. No painel de navegação, escolha Gateways privados virtuais.
2. Escolha Create virtual private gateway (Criar gateway privado virtual).
3. (Opcional) Em Etiqueta de nome, insira um nome para o gateway privado virtual. Ao fazer isso, é criada uma tag com a chave Name e o valor especificado.
4. Em Número de sistema autônomo (ASN), mantenha a seleção padrão, ASN padrão da Amazon, para usar o ASN padrão da Amazon. Caso contrário, selecione Custom ASN (Personalizar ASN) e insira um valor. Para um ASN de 16 bits, o valor deve estar no intervalo de 64512 a 65534. Para um ASN de 32 bits, o valor deve estar no intervalo de 4200000000 a 4294967294.
5. Escolha Create virtual private gateway (Criar gateway privado virtual).

6. Selecione o gateway privado virtual e, depois, escolha Actions (Ações), Attach to VPC (Anexar à VPC).
7. Em VPCs disponíveis, escolha a VPC e selecione Anexar à VPC.

Para criar um gateway privado virtual usando a linha de comando ou a API

- [CreateVpnGateway](#)(API de consulta do Amazon EC2)
- [create-vpn-gateway](#) (AWS CLI)
- [New-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

Para anexar um gateway privado virtual a uma VPC usando a linha de comando ou a API

- [AttachVpnGateway](#)(API de consulta do Amazon EC2)
- [attach-vpn-gateway](#) (AWS CLI)
- [Add-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

Criar um gateway de trânsito

Para obter mais informações sobre como criar um gateway de trânsito, consulte [Gateways de trânsito](#) em Gateways de trânsito da Amazon VPC.

Etapa 3: configurar o roteamento

Para permitir que as instâncias na VPC acessem o gateway do cliente, é necessário configurar a tabela de rotas para incluir as rotas usadas pela conexão VPN e apontá-las para o gateway privado virtual ou o gateway de trânsito.

(Gateway privado virtual) Habilitar a propagação de rotas na tabela de rotas

É possível habilitar a propagação de rotas para a tabela de rotas a fim de propagar rotas da VPN local a local automaticamente.

Para o roteamento estático, os prefixos IP estáticos especificados para a configuração VPN serão propagados para a tabela de rotas sempre que o status da conexão VPN for UP. Da mesma forma, para o roteamento dinâmico, as rotas anunciadas no BGP a partir do gateway do cliente também serão propagadas para a tabela de rotas sempre que o status da conexão VPN for UP.

Note

Se a conexão for interrompida, mas a conexão VPN permanecer no estado UP, todas as rotas propagadas que estão na tabela de rotas não serão removidas automaticamente. Tenha isso em mente se, por exemplo, você quiser que o tráfego faça failover para uma rota estática. Nesse caso, talvez seja necessário desabilitar a propagação de rotas para remover as rotas propagadas.

Para ativar a propagação de rotas usando o console

1. No painel de navegação, escolha Route tables.
2. Selecione a tabela de rotas associada à sub-rede.
3. Na guia Propagação de rotas, selecione Editar propagação de rotas. Selecione o gateway privado virtual que você criou no procedimento anterior e escolha Salvar.

Note

Se você não habilitar a propagação de rotas, será necessário inserir manualmente as rotas estáticas usadas pela conexão VPN. Para fazer isso, selecione a tabela de rotas, escolha Routes (Rotas), Edit (Editar). Em Destination (Destino), adicione a rota estática usada pela conexão de VPN de local a local. Em Destination (Destino), selecione o ID do gateway privado virtual, e escolha Save (Salvar).

Para desativar a propagação de rotas usando o console

1. No painel de navegação, escolha Route tables.
2. Selecione a tabela de rotas associada à sub-rede.
3. Na guia Propagação de rotas, selecione Editar propagação de rotas. Limpe a caixa de seleção Propagar do gateway privado virtual.
4. Escolha Salvar.

Para ativar a propagação de rotas usando a linha de comando ou a API

- [EnableVgwRoutePropagation](#)(API de consulta do Amazon EC2)

- [enable-vgw-route-propagation](#) (AWS CLI)
- [Enable-EC2VgwRoutePropagation](#) (AWS Tools for Windows PowerShell)

Para desativar a propagação de rotas usando a linha de comando ou a API

- [DisableVgwRoutePropagation](#)(API de consulta do Amazon EC2)
- [disable-vgw-route-propagation](#) (AWS CLI)
- [Disable-EC2VgwRoutePropagation](#) (AWS Tools for Windows PowerShell)

(Gateway de trânsito) Adicionar uma rota à tabela de rotas

Se você habilitou a propagação da tabela de rotas para o gateway de trânsito, as rotas para o anexo da VPN são propagadas para a tabela de rotas do gateway de trânsito. Para obter mais informações, consulte [Roteamento](#) em Gateways de trânsito da Amazon VPC.

Se você anexar uma VPC ao gateway de trânsito e quiser habilitar recursos na VPC para acessar o gateway do cliente, será necessário adicionar uma rota à tabela de rotas da sub-rede para apontar para o gateway de trânsito.

Para adicionar uma rota a uma tabela de roteamento da VPC

1. No painel de navegação, escolha Tabelas de rotas.
2. Selecione uma tabela de rotas associada à VPC.
3. Na guia Rotas, escolha Editar rotas.
4. Escolha Adicionar rota.
5. Na coluna Destino, insira o intervalo de endereços IP de destino. Em Target (Destino), escolha o gateway de trânsito.
6. Escolha Salvar alterações.

Etapa 4: atualizar o grupo de segurança

Para permitir acesso às instâncias na VPC de sua rede, você deve atualizar as regras de grupo de segurança para permitir o acesso SSH, RDP e ICMP de entrada.

Como adicionar regras ao grupo de segurança para permitir o acesso

1. No painel de navegação, selecione Grupos de segurança.
2. Selecione o grupo de segurança para as instâncias em sua VPC às quais você deseja permitir acesso.
3. Na guia Regras de entrada, selecione Editar regras de entrada.
4. Adicione as regras que permitem acesso SSH, RDP e ICMP de entrada da rede e selecione Salvar regras. Para obter mais informações, consulte [Regras de grupos de segurança](#) no Guia do usuário da Amazon VPC.

Etapa 5: criar uma conexão VPN

Para criar a conexão VPN, use o gateway do cliente com o gateway privado virtual ou o gateway de trânsito criado anteriormente.

Para criar uma conexão VPN

1. No painel de navegação, selecione Conexões VPN de local a local.
2. Escolha Create VPN Connection (Criar conexão VPN).
3. (Opcional) Em Etiqueta de nome, insira um nome para a conexão VPN. Ao fazer isso, é criada uma marcação com a chave de Name e o valor que você especificar.
4. Em Target gateway type (Tipo de gateway de destino), selecione Virtual private gateway (Gateway privado virtual) ou Transit gateway (Gateway de trânsito). Depois, selecione o gateway privado virtual ou o gateway de trânsito criado anteriormente.
5. Em Gateway do cliente, selecione Existente e, depois, escolha o gateway do cliente criado anteriormente em ID do gateway do cliente.
6. Escolha uma das opções de roteamento dependendo se o seu dispositivo de gateway do cliente oferece suporte ao Border Gateway Protocol (BGP):
 - Se o dispositivo de gateway do cliente oferecer suporte ao BGP, selecione Dynamic (requires BGP) (Dinâmico [requer BGP]).
 - Se o dispositivo de gateway do cliente não oferecer suporte ao BGP, selecione Static (Estático). Em Static IP Prefixes (Prefixos do IP estático), especifique cada prefixo IP para a rede privada da conexão VPN.

7. Se o seu tipo de gateway de destino for de trânsito, em Versão IP de túnel interno, especifique se os túneis de VPN são compatíveis com tráfego IPv4 ou IPv6. O tráfego IPv6 só é compatível com conexões VPN em um gateway de trânsito.
8. Se você especificou IPv4 para túnel dentro da versão IP, você pode, opcionalmente, especificar os intervalos de CIDR IPv4 para o gateway do cliente e AWS os lados que têm permissão para se comunicar pelos túneis VPN. O padrão é `0.0.0.0/0`.

Se você especificou IPv6 para túnel dentro da versão IP, você pode, opcionalmente, especificar os intervalos de CIDR IPv6 para o gateway do cliente e AWS os lados que têm permissão para se comunicar pelos túneis VPN. O padrão para ambos os intervalos é `::/0`.

9. Para o tipo de endereço IP externo, mantenha a opção padrão, `PublicIpv4`.
10. (Opcional) Em Opções de túnel, é possível especificar as seguintes informações para cada túnel:
 - Um bloco CIDR do IPv4 de tamanho /30 do intervalo `169.254.0.0/16` para os endereços IPv4 do túnel interno.
 - Se você especificou IPv6 em Versão IP de túnel interno, um bloco CIDR do IPv6 /126 do intervalo `fd00::/8` para os endereços IPv6 do túnel interno.
 - A chave pré-compartilhada do IKE (PSK). As seguintes versões são compatíveis: IKEv1 ou IKEv2.
 - Para editar as opções avançadas do túnel, escolha Editar opções de túnel. Para ter mais informações, consulte [Opções de túnel VPN](#).
11. Escolha Create VPN Connection (Criar conexão VPN). Pode levar alguns minutos para criar a conexão VPN.

Para criar uma conexão VPN usando a linha de comando ou a API

- [CreateVpnConnection](#) (API de consulta do Amazon EC2)
- [create-vpn-connection](#) (AWS CLI)
- [New-EC2VpnConnection](#) (AWS Tools for Windows PowerShell)

Etapa 6: baixar o arquivo de configuração

Depois de criar a conexão VPN, você poderá baixar um arquivo de configuração de exemplo para usar na configuração do dispositivo de gateway do cliente.

Important

O arquivo de configuração é apenas um exemplo e pode não corresponder totalmente às configurações da conexão VPN pretendidas. Ele especifica os requisitos mínimos para uma conexão VPN do grupo AES128, SHA1 e Diffie-Hellman 2 na maioria das AWS regiões e do grupo 14 do AES128, SHA2 e Diffie-Hellman nas regiões. AWS GovCloud Ele também especifica chaves pré-compartilhadas para autenticação. É necessário modificar o arquivo de configuração de exemplo para usufruir dos algoritmos de segurança adicionais, grupos Diffie-Hellman, certificados privados e tráfego IPv6.

Introduzimos o suporte a IKEv2 nos arquivos de configuração para muitos dispositivos de gateway de clientes populares e continuaremos a adicionar novos arquivos ao longo do tempo. Para obter uma lista de arquivos de configuração compatível com IKEv2, consulte [dispositivo de gateway do cliente](#).

Permissões

Para carregar adequadamente a tela de configuração de download a partir do AWS Management Console, você deve garantir que sua função ou usuário do IAM tenha permissão para as seguintes APIs do Amazon EC2: `GetVpnConnectionDeviceTypes` e `GetVpnConnectionDeviceSampleConfiguration`

Como baixar o arquivo de configuração usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão VPN e escolha Fazer download da configuração.
4. Escolha o Fornecedor, a Plataforma, o Software e a Versão IKE que correspondem ao dispositivo do gateway do cliente. Se o dispositivo não estiver listado, selecione Genérico (Genérico).
5. Escolha Download.

Para baixar um arquivo de configuração de exemplo usando a linha de comando ou API da

- [GetVpnConnectionDeviceTypes](#)(API do Amazon EC2)
- [GetVpnConnectionDeviceSampleConfiguration](#)(API de consulta do Amazon EC2)
- [get-vpn-connection-device-tipos](#) (AWS CLI)

- [get-vpn-connection-device-configuração de amostra \(\)](#)AWS CLI

Etapa 7: configurar o dispositivo de gateway do cliente

Use o arquivo de configuração de exemplo para configurar os dispositivos de gateway do cliente. O dispositivo de gateway do cliente é o dispositivo físico ou software situado no seu lado da conexão VPN. Para ter mais informações, consulte [O dispositivo de gateway do cliente](#).

Arquiteturas site a site VPN

Vários cenários VPN de conexão

A seguir estão os cenários nos quais você pode criar várias VPN conexões com um ou mais dispositivos de gateway do cliente.

Várias VPN conexões usando o mesmo dispositivo de gateway do cliente

Você pode criar VPN conexões adicionais de sua localização local para outras VPCs usando o mesmo dispositivo de gateway do cliente. Você pode reutilizar o mesmo endereço IP do gateway do cliente para cada uma dessas VPN conexões.

VPNConexão redundante usando um segundo dispositivo de gateway do cliente

Para se proteger contra a perda de conectividade se o dispositivo de gateway do cliente ficar indisponível, você pode configurar uma segunda VPN conexão usando um segundo dispositivo de gateway do cliente. Para obter mais informações, consulte [Utilização de conexões do Site-to-Site VPN redundantes para realizar failover](#). Ao estabelecer dispositivos de gateway do cliente redundantes em uma única localização, os dois dispositivos devem anunciar os mesmos intervalos de IP.

Vários dispositivos de gateway do cliente em um único gateway privado virtual (AWS VPN CloudHub)

Você pode estabelecer várias VPN conexões com um único gateway privado virtual a partir de vários dispositivos de gateway do cliente. Isso permite que você tenha vários locais conectados ao AWS VPN CloudHub. Para obter mais informações, consulte [Fornecendo comunicação segura entre sites usando VPN CloudHub](#). Quando há dispositivos de gateway do cliente em várias localizações geográficas, cada dispositivo deve anunciar um conjunto exclusivo de intervalos de IP específicos da localização.

A seguir estão as arquiteturas comuns de site a site: VPN

- [the section called “Conexões VPN única e múltipla”](#)
- [the section called “Conexões VPN redundantes”](#)
- [the section called “AWS VPN CloudHub”](#)

Exemplos de conexão VPN única e múltipla do Site-to-Site VPN

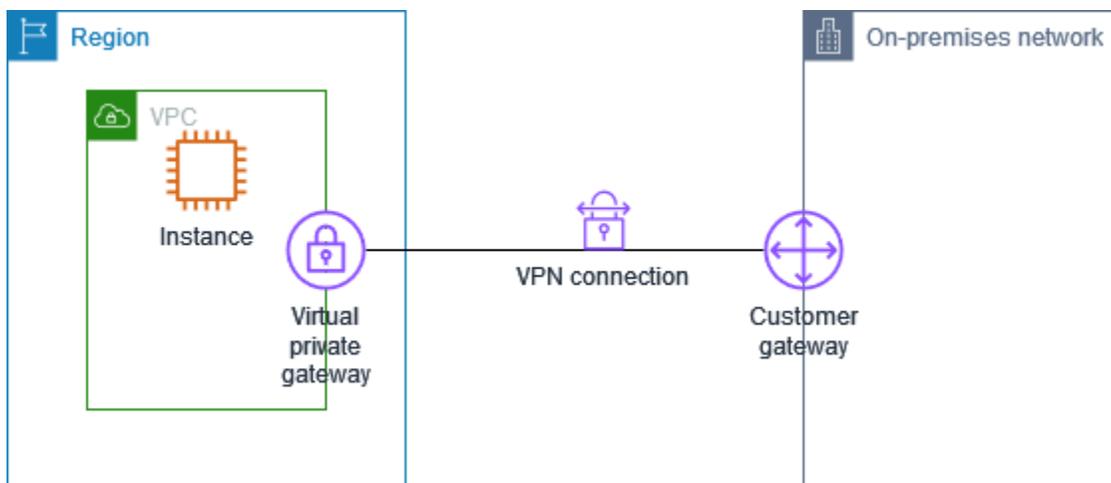
Os diagramas a seguir exibem tanto uma única como várias conexões do Site-to-Site VPN.

Exemplos

- [Conexão única do Site-to-Site VPN](#)
- [Conexão única do Site-to-Site VPN com um gateway de trânsito](#)
- [Várias conexões do Site-to-Site VPN](#)
- [Várias conexões do Site-to-Site VPN com um gateway de trânsito](#)
- [Conexão VPN site-to-site com AWS Direct Connect](#)
- [Conexão VPN de site a site com IP privado com AWS Direct Connect](#)

Conexão única do Site-to-Site VPN

A VPC tem um gateway privado virtual anexado, e a rede on-premises (remota) inclui um dispositivo de gateway do cliente que precisa ser configurado para habilitar a conexão VPN. É necessário atualizar as tabelas de rotas da VPC para que qualquer tráfego da VPC vinculado à rede vá para o gateway privado virtual.

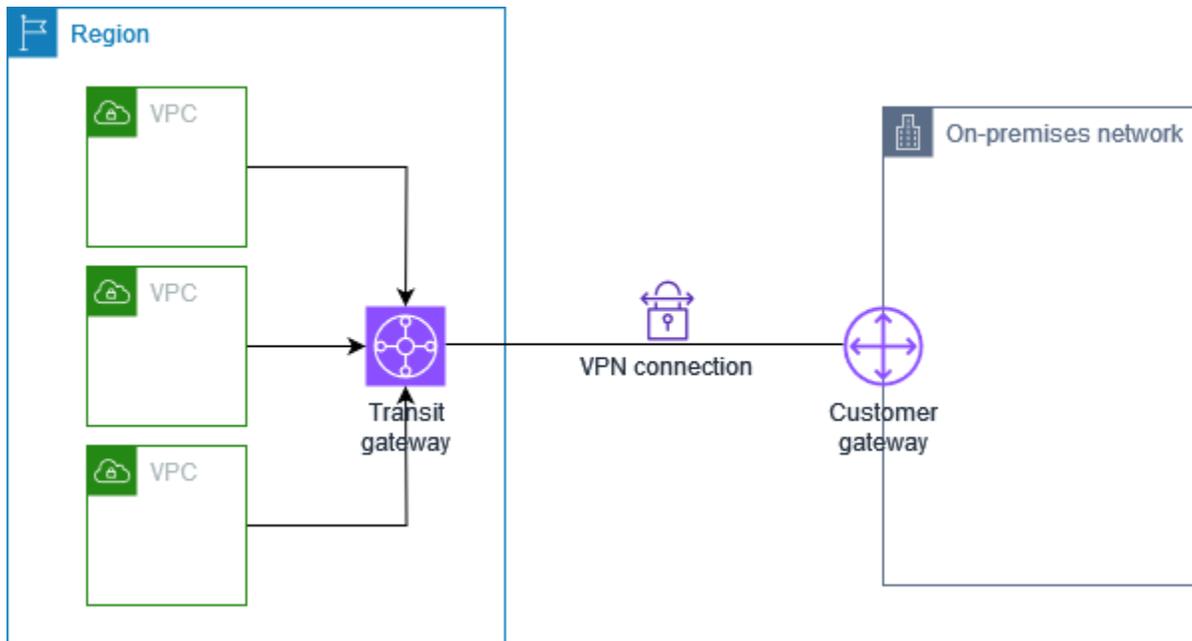


Para conhecer as etapas para configurar esse cenário, consulte [Começando com AWS Site-to-Site VPN](#).

Conexão única do Site-to-Site VPN com um gateway de trânsito

A VPC tem um gateway de trânsito anexado, e a rede on-premises (remota) inclui um dispositivo de gateway do cliente que precisa ser configurado para habilitar a conexão VPN. É necessário atualizar

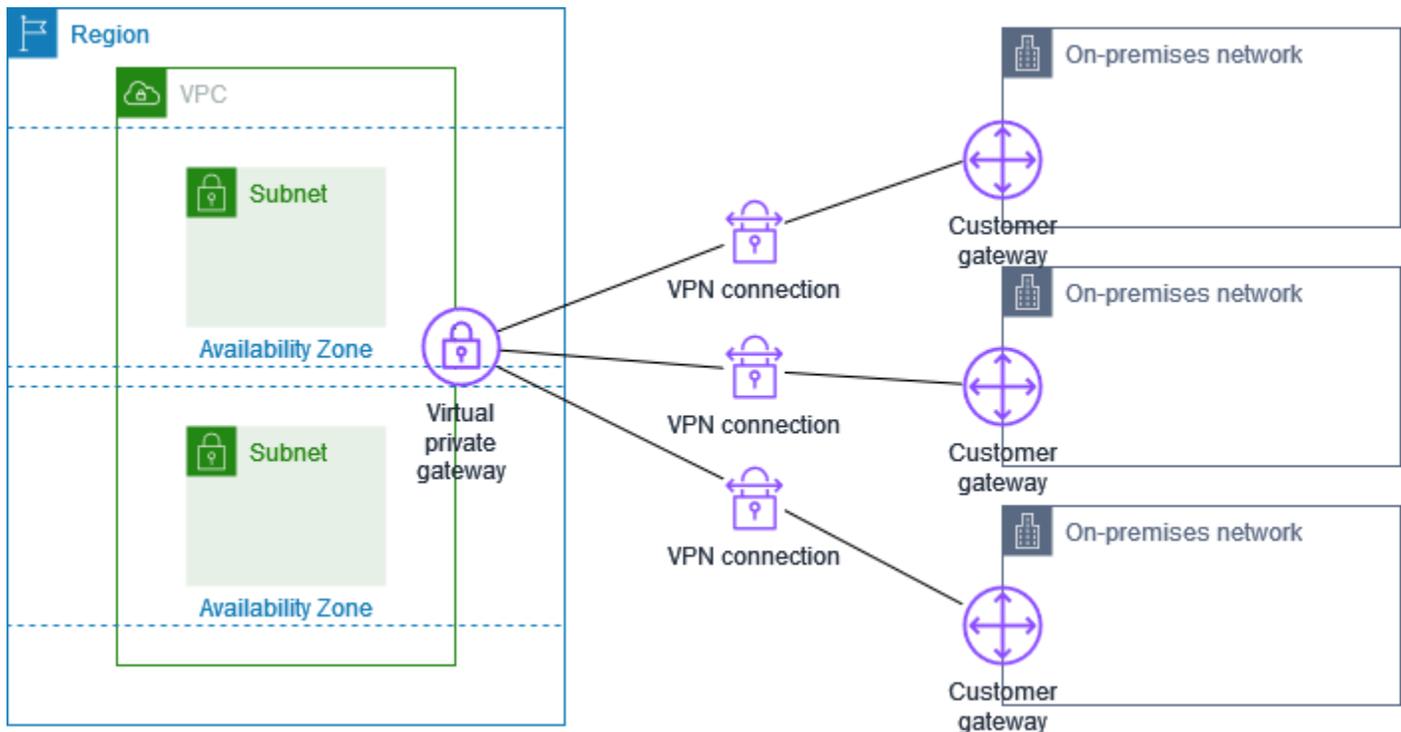
as tabelas de rota da VPC para que qualquer tráfego da VPC vinculado à rede vá para o gateway de trânsito.



Para conhecer as etapas para configurar esse cenário, consulte [Começando com AWS Site-to-Site VPN](#).

Várias conexões do Site-to-Site VPN

A VPC tem um gateway privado virtual anexado e você tem várias conexões do Site-to-Site VPN a várias localidades no local. Configure o roteamento para que qualquer tráfego da VPC vinculado às redes seja roteado para o gateway privado virtual.

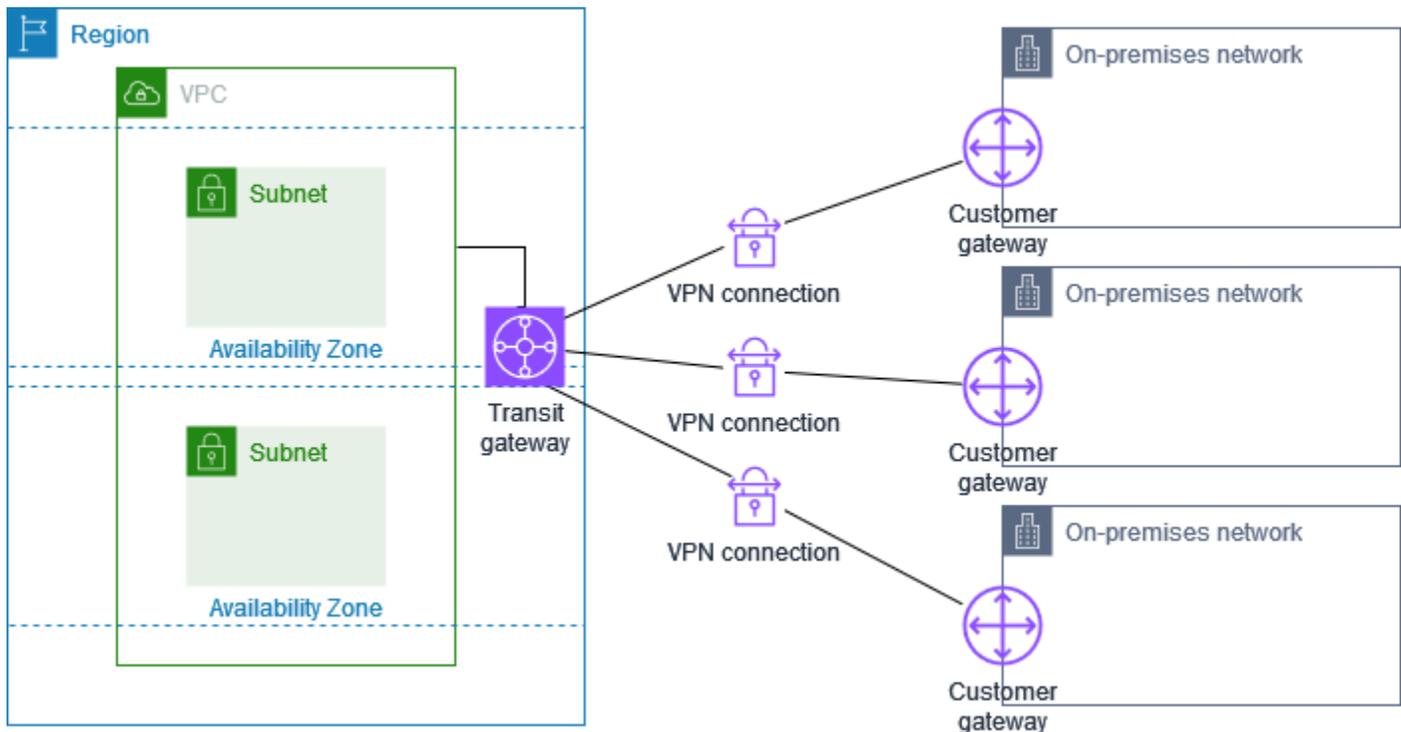


Ao estabelecer várias conexões do Site-to-Site VPN para uma única VPC, é possível configurar um segundo gateway do cliente e, assim, criar uma conexão redundante para o mesmo local externo. Para ter mais informações, consulte [Utilização de conexões do Site-to-Site VPN redundantes para realizar failover](#).

Você também pode usar esse cenário para criar conexões do Site-to-Site VPN com várias localizações geográficas e fornecer comunicação segura entre sites. Para ter mais informações, consulte [Fornecendo comunicação segura entre sites usando VPN CloudHub](#).

Várias conexões do Site-to-Site VPN com um gateway de trânsito

A VPC tem um gateway de trânsito anexado e você tem várias conexões do Site-to-Site VPN para vários locais. Configure o roteamento para que qualquer tráfego da VPC vinculado às suas redes seja roteado para o gateway de trânsito.

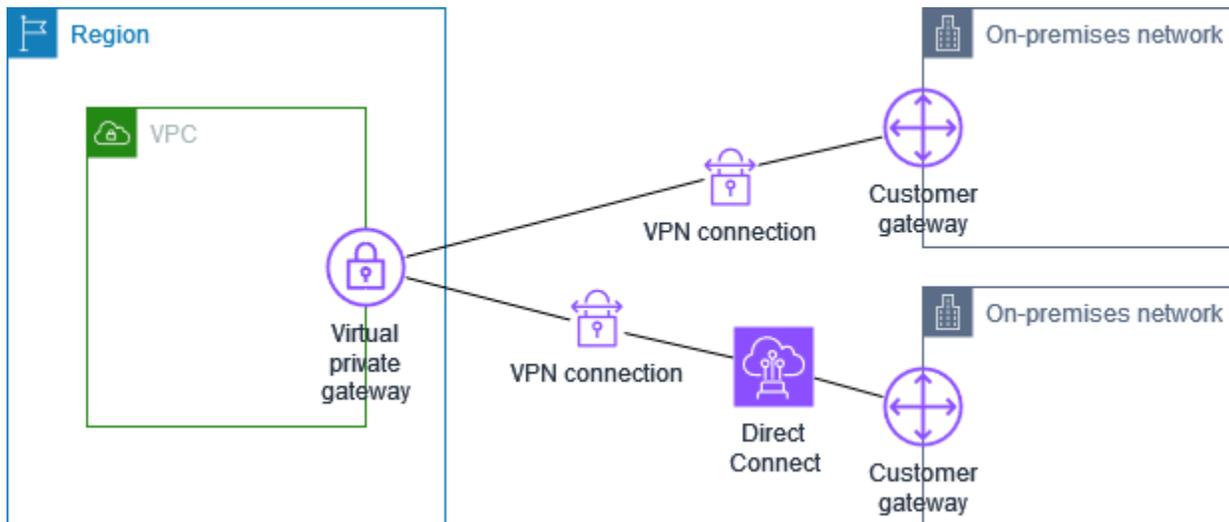


Ao estabelecer várias conexões do Site-to-Site VPN para um único gateway de trânsito, é possível configurar um segundo gateway do cliente e, assim, criar uma conexão redundante para o mesmo local externo.

Você também pode usar esse cenário para criar conexões do Site-to-Site VPN com várias localizações geográficas e fornecer comunicação segura entre sites.

Conexão VPN site-to-site com AWS Direct Connect

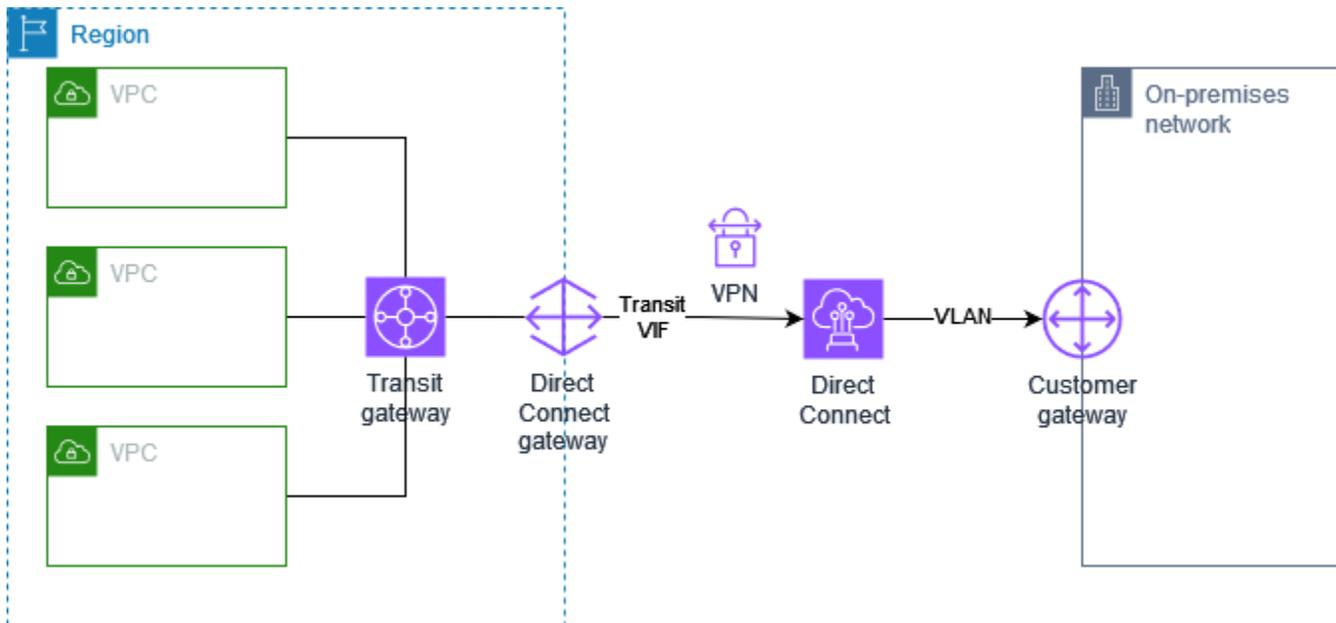
A VPC tem um gateway privado virtual conectado e se conecta à sua rede local (remota) por meio de. AWS Direct Connect Você pode configurar uma interface virtual AWS Direct Connect pública para estabelecer uma conexão de rede dedicada entre sua rede e AWS recursos públicos por meio de um gateway privado virtual. Você configura o roteamento para que qualquer tráfego da VPC vinculado à sua rede seja direcionado para o gateway privado virtual e AWS Direct Connect para a conexão.



Quando ambas AWS Direct Connect e a conexão VPN estão configuradas no mesmo gateway privado virtual, adicionar ou remover objetos pode fazer com que o gateway privado virtual entre no estado de 'anexação'. Isso indica que uma alteração está sendo feita no roteamento interno que alternará entre o AWS Direct Connect e a conexão VPN para minimizar interrupções e perda de pacotes. Quando isso estiver concluído, o gateway privado virtual retorna ao estado "anexado".

Conexão VPN de site a site com IP privado com AWS Direct Connect

Com uma VPN IP privada Site-to-Site, você pode AWS Direct Connect criptografar o tráfego entre sua rede AWS local sem o uso de endereços IP públicos. A VPN IP privada AWS Direct Connect garante que o tráfego entre redes locais AWS e redes locais seja seguro e privado, permitindo que os clientes cumpram as exigências regulatórias e de segurança.



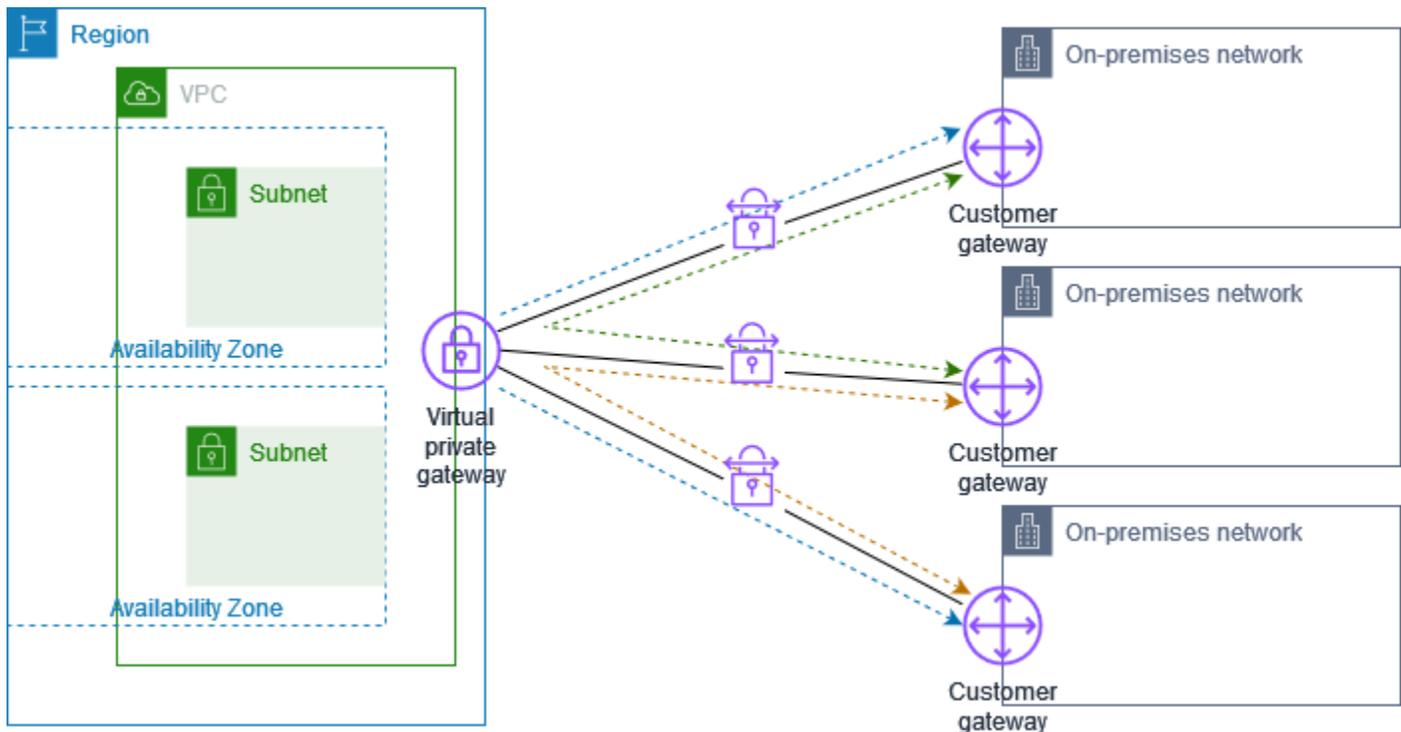
Para obter mais informações, consulte a seguinte postagem no blog: [Apresentando VPNs IP AWS Site-to-Site VPN privadas](#).

Fornecendo comunicação segura entre sites usando VPN CloudHub

Se você tiver várias AWS Site-to-Site VPN conexões, poderá fornecer comunicação segura entre sites usando a AWS VPN CloudHub. Isso permite que os sites comuniquem-se entre si e não somente com os recursos na VPC. A VPN CloudHub opera em um hub-and-spoke modelo simples que você pode usar com ou sem uma VPC. Esse design é adequado se você tiver várias filiais e conexões de Internet existentes e quiser implementar um hub-and-spoke modelo conveniente e potencialmente de baixo custo para conectividade primária ou de backup entre esses locais.

Visão geral

O diagrama a seguir mostra a CloudHub arquitetura da VPN. As linhas tracejadas mostram o tráfego de rede entre sites remotos roteado pelas conexões VPN. Os sites não devem ter intervalos de IP sobrepostos.



Para este cenário, faça o seguinte:

1. Crie um único gateway privado virtual.
2. Crie vários gateways do cliente, cada um com o endereço IP público do gateway. Você deve usar um número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) exclusivo para cada gateway do cliente.
3. Crie uma conexão do Site-to-Site VPN encaminhada dinamicamente de cada gateway do cliente com um gateway privado virtual comum.
4. Configure cada dispositivo de gateway do cliente para anunciar um prefixo específico do site (como 10.0.0.0/24, 10.0.1.0/24) para o gateway privado virtual. Esses anúncios de roteamento são recebidos e novamente anunciados para cada ponto BGP, permitindo o envio e o recebimento de dados entre os sites. Isso é feito por meio das instruções da rede, localizadas nos arquivos de configuração para a conexão do Site-to-Site VPN. As instruções da rede diferem ligeiramente, dependendo do tipo de roteador usado.
5. Configure as rotas em suas tabelas de rotas de sub-rede para permitir que as instâncias em sua VPC se comuniquem com seus sites. Para ter mais informações, consulte [\(Gateway privado virtual\) Habilitar a propagação de rotas na tabela de rotas](#). É possível configurar uma rota agregada na tabela de rotas (por exemplo, 10.0.0.0/16). Use prefixos mais específicos entre os dispositivos de gateway do cliente e o gateway privado virtual.

Sites que usam AWS Direct Connect conexões com o gateway privado virtual também podem fazer parte da AWS VPN CloudHub. Por exemplo, a sede corporativa em Nova York pode ter uma conexão AWS Direct Connect com a VPC, enquanto as filiais usam as conexões Site-to-Site VPN para a VPC. As filiais em Los Angeles e Miami podem enviar e receber dados umas com as outras e com a sede da sua empresa, todas usando a AWS VPN CloudHub.

Definição de preço

Para usar a AWS VPN CloudHub, você paga taxas de conexão VPN Site-to-Site típicas da Amazon VPC. A quantia devida pela taxa de conexão é calculada pelo total de horas em que cada VPN esteve conectada ao gateway privado virtual. Quando você envia dados de um site para outro usando a AWS VPN CloudHub, não há custo para enviar dados do seu site para o gateway privado virtual. Pague somente as taxas de transferência de dados da AWS padrão em função da retransmissão dos dados do gateway privado virtual para o endpoint.

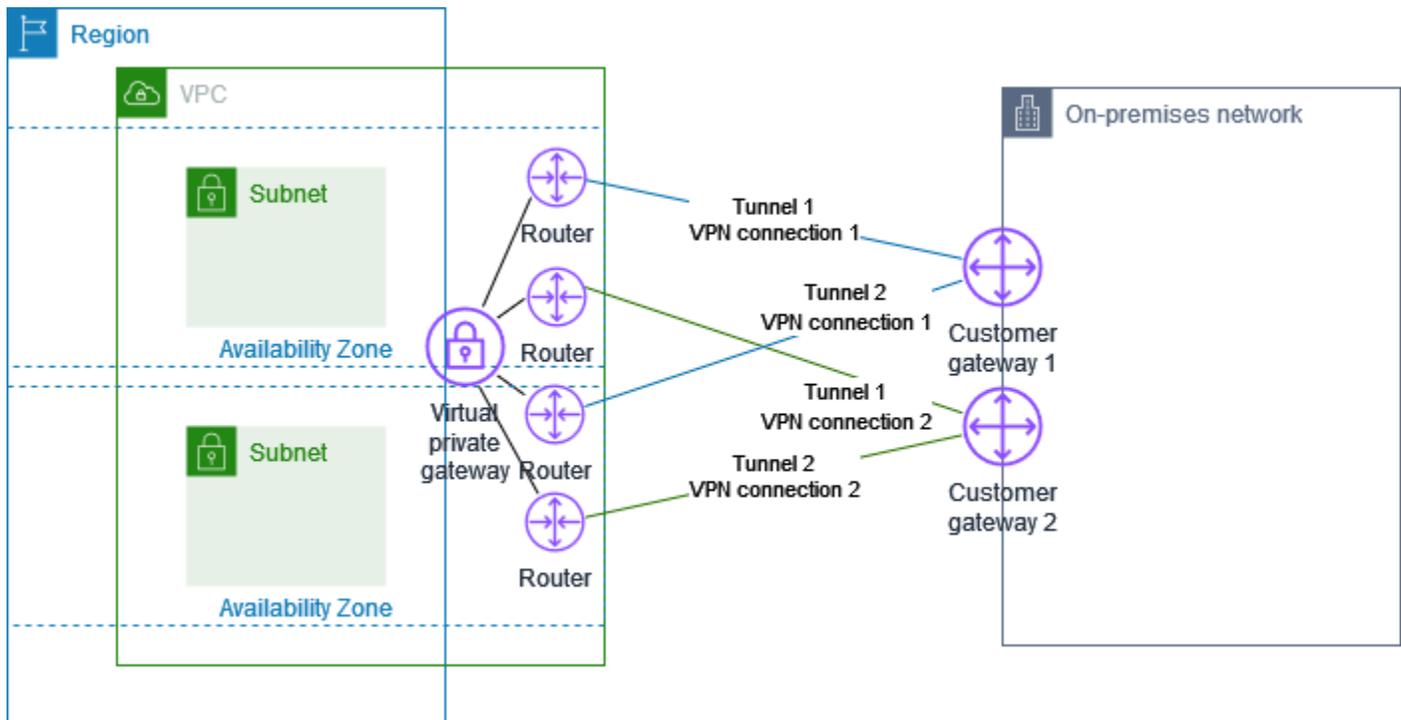
Por exemplo, se você tiver um site em Los Angeles e um segundo site em Nova York, e ambos os sites tiverem uma conexão do Site-to-Site VPN com o gateway privado virtual, você pagará a taxa por hora para cada conexão do Site-to-Site VPN (portanto, se a taxa fosse de 0,05 USD por hora, a cobrança total será de 0,10 USD por hora). Você também paga as taxas de transferência de AWS dados padrão para todos os dados enviados de Los Angeles para Nova York (e vice-versa) que atravessam cada conexão VPN Site-to-Site. O tráfego de rede enviado pela conexão VPN Site-to-Site para o gateway privado virtual é gratuito, mas o tráfego de rede enviado pela conexão VPN Site-to-Site do gateway privado virtual para o endpoint é cobrado de acordo com a taxa de transferência de dados padrão. AWS

Para obter mais informações, consulte [Definição de preço da conexão do Site-to-Site VPN](#).

Utilização de conexões do Site-to-Site VPN redundantes para realizar failover

A indisponibilidade do gateway do cliente acarreta a perda de conectividade. Para se proteger, adicione um segundo gateway do cliente e configure uma segunda conexão do Site-to-Site VPN à sua VPC e para o gateway privado virtual. O uso de conexões VPN e dispositivos de gateway do cliente redundantes permite executar a manutenção de um dos gateways enquanto o tráfego flui por meio da conexão VPN do segundo gateway do cliente.

O diagrama a seguir mostra as duas conexões VPN. Cada conexão VPN tem seus próprios túneis e seu próprio gateway do cliente.



Para este cenário, faça o seguinte:

- Configure uma segunda conexão do Site-to-Site VPN usando o mesmo gateway privado virtual e criando um gateway do cliente. O endereço IP do gateway do cliente para a segunda conexão do Site-to-Site VPN deve ser acessível ao público.
- Configure um segundo dispositivo de gateway do cliente. Os dois dispositivos devem anunciar os mesmos intervalos de IP para o gateway privado virtual. Usamos o roteamento BGP a fim de determinar o caminho para o tráfego. Se ocorrer uma falha no dispositivo de gateway do cliente, o gateway privado virtual direcionará todo o tráfego para o dispositivo de gateway do cliente em funcionamento.

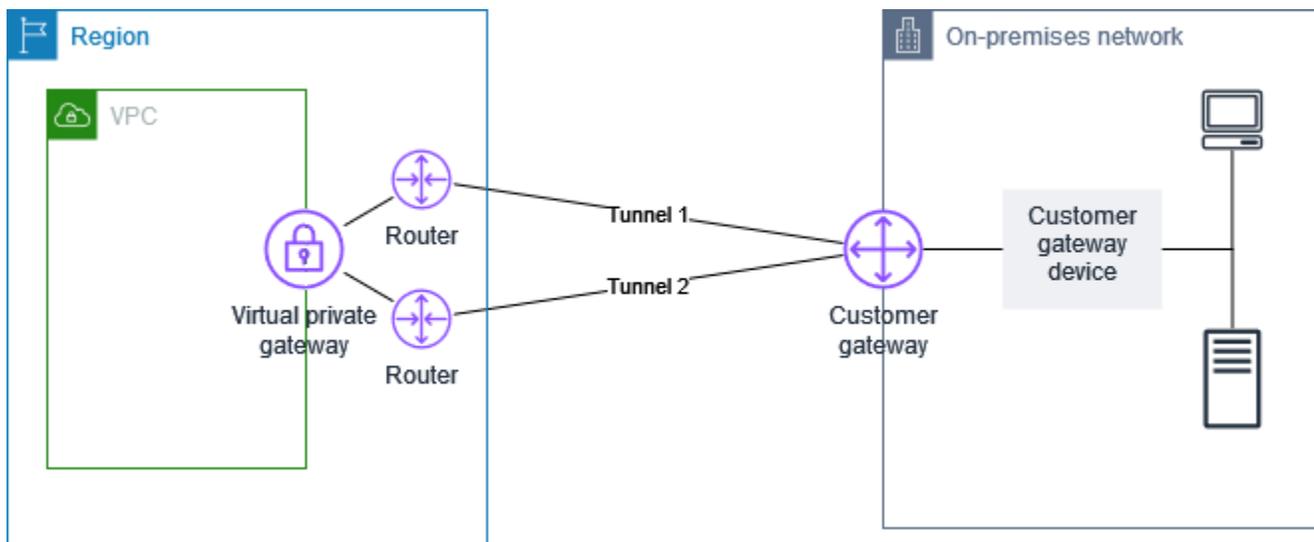
As conexões do Site-to-Site VPN roteadas dinamicamente usam o Border Gateway Protocol (BGP) para trocar informações de roteamento entre os gateways do cliente e os gateways privados virtuais. As conexões do Site-to-Site VPN roteadas estaticamente requerem que as rotas estáticas sejam inseridas na rede remota situada no seu lado do gateway do cliente. As informações de rotas anunciadas em BGP e estaticamente inseridas permitem os gateways em ambos os lados, indicando a disponibilidade dos túneis e redirecionando o tráfego, caso ocorra uma falha. Recomendamos que configure a rede para usar as informações de roteamento fornecidas pelo BGP (se disponível) e, assim, selecionar um caminho disponível. A configuração exata depende da arquitetura da rede.

Para obter mais informações sobre como criar e configurar um gateway do cliente e uma conexão do Site-to-Site VPN, consulte [Começando com AWS Site-to-Site VPN](#).

O dispositivo de gateway do cliente

Um dispositivo de gateway do cliente é um dispositivo físico ou de software que você possui ou gerencia em sua rede local (do seu lado de uma conexão site a siteVPN). Você ou seu administrador de rede devem configurar o dispositivo para funcionar com a conexão site a site. VPN

O diagrama a seguir mostra sua rede, o dispositivo de gateway do cliente e a VPN conexão que vai para o gateway privado virtual conectado à suaVPC. As duas linhas entre o gateway do cliente e o gateway privado virtual representam os túneis da VPN conexão. Se houver uma falha no dispositivo AWS, sua VPN conexão automaticamente passará para o segundo túnel para que seu acesso não seja interrompido. De tempos em tempos, AWS também realiza manutenção de rotina na VPN conexão, o que pode desativar brevemente um dos dois túneis da sua VPN conexão. Para obter mais informações, consulte [Substituições de endpoint de túnel Site-to-Site VPN](#). É importante configurar o dispositivo de gateway do cliente para usar os dois túneis.



Para obter as etapas para configurar uma VPN conexão, consulte [Começando com AWS Site-to-Site VPN](#). Durante esse processo, você cria um recurso de gateway do cliente no AWS, que fornece informações AWS sobre seu dispositivo, por exemplo, seu endereço IP público. Para obter mais informações, consulte [Opções de gateway do cliente para a conexão de VPN de local a local](#). O recurso de gateway do cliente em AWS não configura nem cria o dispositivo de gateway do cliente. Você precisará configurar o dispositivo por conta própria.

Você também pode encontrar VPN dispositivos de software no [AWS Marketplace](#).

Requisitos do seu dispositivo de gateway do cliente

Se você tiver um dispositivo que não esteja na lista de exemplos anterior, esta seção descreve os requisitos que o dispositivo deve atender para que você possa usá-lo para estabelecer uma conexão site a site VPN.

Há quatro etapas principais para a configuração do seu dispositivo de gateway do cliente. Os símbolos a seguir representam cada parte da configuração.

IKE	Associação de segurança do Internet Key Exchange (IKE). Isso é necessário para trocar as chaves usadas para estabelecer a associação IPsec de segurança.
IPsec	IPsec associação de segurança. Isso lida com a criptografia do túnel, com a autenticação e assim por diante.
Tunnel	Interface do túnel. Isso recebe tráfego de e para o túnel.
BGP	(Opcional) Emparelhamento do Border Gateway Protocol (BGP). Para dispositivos que usam BGP, isso troca rotas entre o dispositivo de gateway do cliente e o gateway privado virtual.

A tabela a seguir lista os requisitos do dispositivo de gateway do cliente, os relacionados RFC (para referência) e os comentários sobre os requisitos.

Cada VPN conexão consiste em dois túneis separados. Cada túnel contém uma associação IKE de segurança, uma associação IPsec de segurança e um BGP peering. Você está limitado a um par exclusivo de associação de segurança (SA) por túnel (um de entrada e um de saída) e, portanto, a dois pares de SA exclusivos no total para dois túneis (quatro). Alguns dispositivos usam uma política baseada em políticas VPN e criam SAs tantas ACL entradas. Assim, talvez seja necessário consolidar as regras e, depois, filtrar para não permitir o tráfego indesejado.

Por padrão, o VPN túnel aparece quando o tráfego é gerado e a IKE negociação é iniciada do seu lado da VPN conexão. Em vez disso, você pode configurar a VPN conexão para iniciar a IKE negociação pelo AWS lado da conexão. Para obter mais informações, consulte [Opções de iniciação de túnel do Site-to-Site VPN](#).

VPNs endpoints oferecem suporte à chave e podem iniciar renegociações quando a fase 1 estiver prestes a expirar, caso o dispositivo de gateway do cliente não tenha enviado nenhum tráfego de renegociação.

Requisito	RFC	Comentários
Estabelecer associação IKE de segurança <div style="background-color: #FFD700; padding: 2px; display: inline-block; margin-top: 5px;">IKE</div>	RFC2409 RFC7296	<p>A associação IKE de segurança é estabelecida primeiro entre o gateway privado virtual e o dispositivo de gateway do cliente usando uma chave pré-compartilhada ou um certificado privado usado AWS Private Certificate Authority como autenticador. Quando estabelecido, IKE negocia uma chave efêmera para proteger futuras mensagens. IKE Deve haver um acordo completo entre os parâmetros, incluindo parâmetros de criptografia e de autenticação.</p> <p>Ao criar uma VPN conexão em AWS, você pode especificar sua própria chave pré-compartilhada para cada túnel ou deixar AWS gerar uma para você. Como alternativa, você pode especificar o certificado privado usado AWS Private Certificate Authority para usar em seu dispositivo de gateway do cliente. Para obter mais informações, sobre a configuração de VPN túneis, consulte. Opções de túnel para a conexão do Site-to-Site VPN</p> <p>As seguintes versões são suportadas: IKEv1 IKEv2 e. Suportamos o modo principal somente comIKEv1.</p> <p>O VPN serviço Site-to-Site é uma solução baseada em rotas. Se você estiver usando uma configuração com base em políticas, limite a configuração a uma única associação de segurança (SA).</p>
Estabeleça associações de IPsec segurança no modo Túnel	RFC4301	Usando a chave IKE efêmera, as chaves são estabelecidas entre o gateway privado virtual e o dispositivo de gateway do cliente para formar uma

Requisito	RFC	Comentários
IPsec		associação de IPsec segurança (SA). O tráfego entre os gateways é criptografado e descryptografado usando essa SA. As chaves efêmeras usadas para criptografar o tráfego dentro do IPsec SA são alternadas automaticamente regularmente para garantir a IKE confidencialidade das comunicações.
Use a função de criptografia de AES 128 bits ou AES 256 bits	RFC3602	A função de criptografia é usada para garantir a privacidade IKE e as associações IPsec de segurança.
Use a função de hash SHA -1 ou SHA -2 (256)	RFC2404	Essa função de hash é usada para autenticar associações IKE e associações de IPsec segurança.
Use o Diffie-Hellman Perfect Forward Secrecy.	RFC2409	<p>IKE usa o Diffie-Hellman para estabelecer chaves efêmeras para proteger toda a comunicação entre os dispositivos de gateway do cliente e os gateways privados virtuais.</p> <p>Os seguintes grupos são compatíveis:</p> <ul style="list-style-type: none"> • Grupos da fase 1: 2, 14-24 • Grupos da fase 2: 2, 5, 14-24
(VPN Conexões roteadas dinamicamente) Use Dead Peer Detection IPsec	RFC3706	O Dead Peer Detection permite que os VPN dispositivos identifiquem rapidamente quando uma condição de rede impede a entrega de pacotes pela Internet. Quando isso ocorre, os gateways excluem as associações de segurança e tentam criar outras associações. Durante esse processo, o IPsec túnel alternativo é usado, se possível.

Requisito	RFC	Comentários
(VPNConexões roteadas dinamicamente) Vincule o túnel à interface lógica (baseada em rotas) VPN Tunnel	Nenhum	Seu dispositivo deve ser capaz de vincular o IPsec túnel a uma interface lógica. A interface lógica contém um endereço IP que é usado para estabelecer o BGP emparelhamento para o gateway privado virtual. Essa interface lógica não deve realizar nenhum encapsulamento adicional (por exemplo, GRE ou IP em IP). Sua interface deve ser configurada para uma Unidade de Transmissão Máxima de 1399 bytes ()MTU.
(Conexões roteadas dinamicamenteVPN) Estabeleça peerings BGP BGP	RFC4271	BGPé usado para trocar rotas entre o dispositivo de gateway do cliente e o gateway privado virtual para dispositivos que usamBGP. Todo BGP o tráfego é criptografado e transmitido pela IPsec Security Association. BGPé necessário para que ambos os gateways troquem os prefixos IP que podem ser acessados por meio do SA. IPsec

Uma AWS VPN conexão não é compatível com o Path MTU Discovery ([RFC1191](#)).

Se houver um firewall entre o dispositivo de gateway do cliente e a Internet, consulte [Regras de firewall para seu dispositivo de gateway do cliente](#).

Práticas recomendadas para o dispositivo de gateway do cliente

Use IKEv2

É altamente recomendável usar IKEv2 para sua conexão site a site. VPN IKEv2é um protocolo mais simples, mais robusto e mais seguro do que o. IKEv1 Você só deve usar IKEv1 se o dispositivo de gateway do cliente não for compatívelIKEv2. Para obter mais detalhes sobre as diferenças entre IKEv1 eIKEv2, consulte o [Apêndice A](#) do. RFC7296

Redefinir o sinalizador “Não fragmentar (DF)” nos pacotes

Alguns pacotes carregam um sinalizador chamado de Não fragmentar (DF), que indica que o pacote não deve ser fragmentado. Se os pacotes carregarem o sinalizador, os gateways gerarão uma mensagem ICMP Path MTU Exceeded. Em alguns casos, os aplicativos não contêm mecanismos

adequados para processar essas ICMP mensagens e reduzir a quantidade de dados transmitidos em cada pacote. Alguns VPN dispositivos podem substituir o sinalizador DF e fragmentar pacotes incondicionalmente, conforme necessário. Se o dispositivo de gateway do cliente tiver essa capacidade, recomendamos o uso, conforme apropriado. Consulte [RFC791](#) para obter mais detalhes.

Fragmentar pacotes IP antes da criptografia

Se os pacotes enviados pela sua VPN conexão site a site excederem o MTU tamanho, eles deverão estar fragmentados. Para evitar a diminuição do desempenho, recomendamos que você configure seu dispositivo de gateway do cliente para fragmentar os pacotes antes de serem criptografados. Em seguida, um site a outro VPN reunirá todos os pacotes fragmentados antes de encaminhá-los para o próximo destino, a fim de obter maiores fluxos pela rede. Consulte [RFC4459](#) para obter mais detalhes.

Certifique-se de que o tamanho do pacote não exceda as MTU redes de destino

Como o site a site VPN reunirá todos os pacotes fragmentados recebidos do dispositivo de gateway do cliente antes de encaminhá-los para o próximo destino, lembre-se de que pode haver considerações sobre o tamanho do MTU pacote/considerações para as redes de destino para as quais esses pacotes serão encaminhados em seguida, como por exemplo. AWS Direct Connect

Ajuste MTU e MSS dimensionado de acordo com os algoritmos em uso

TCPs pacotes geralmente são o tipo mais comum de pacote em IPsec túneis. O site a site VPN suporta uma unidade de transmissão máxima (MTU) de 1446 bytes e um tamanho máximo de segmento correspondente (MSS) de 1406 bytes. No entanto, os algoritmos de criptografia têm tamanhos de cabeçalho variados e podem impedir a capacidade de atingir esses valores máximos. Para obter o desempenho ideal evitando a fragmentação, recomendamos que você defina o MTU e MSS com base especificamente nos algoritmos que estão sendo usados.

Use a tabela a seguir para definir seu MTU/MSS para evitar a fragmentação e obter o desempenho ideal:

Algoritmo de criptografia	Algoritmo de hash	NAT-Travessia	MTU	MSS (IPv4)	MSS(IPv6-em-) IPv4
AES- GCM-16	N/D	desabilitado	1446	1406	1386

Algoritmo de criptografia	Algoritmo de hash	NAT-Travessia	MTU	MSS (IPv4)	MSS(IPv6-em-) IPv4
AES- GCM -16	N/D	habilitado	1438	1398	1378
AES-CBC	SHA1/SHA2-256	desabilitado	1438	1398	1378
AES-CBC	SHA1/SHA2-256	habilitado	1422	1382	1362
AES-CBC	SHA2-384	desabilitado	1422	1382	1362
AES-CBC	SHA2-384	habilitado	1422	1382	1362
AES-CBC	SHA2-512	desabilitado	1422	1382	1362
AES-CBC	SHA2-512	habilitado	1406	1366	1346

 Note

Os GCM algoritmos AES - abrangem criptografia e autenticação, portanto, não há uma escolha distinta de algoritmo de autenticação que possa afetar MTU.

Desativar IKE exclusivo IDs

Alguns dispositivos de gateway do cliente oferecem suporte a uma configuração que garante que, no máximo, exista uma associação de segurança de fase 1 por configuração de túnel. Essa configuração pode resultar em estados inconsistentes da Fase 2 entre os VPN pares. Se o dispositivo de gateway do cliente suportar essa configuração, recomendamos desativá-la.

Regras de firewall para seu dispositivo de gateway do cliente

Você deve ter um endereço IP estático para usar como ponto final dos IPsec túneis que conectam seu dispositivo de gateway do cliente aos endpoints. AWS Site-to-Site VPN Se houver um firewall entre AWS e seu dispositivo de gateway do cliente, as regras nas tabelas a seguir devem estar

em vigor para estabelecer os IPsec túneis. Os endereços IP do AWS lado -estarão no arquivo de configuração.

Entrada (pela Internet)

Regra de entrada I1

IP de origem	IP externo do túnel 1
Dest IP	Gateway do cliente
Protocolo	UDP
Porta de origem	500
Destino	500

Regra de entrada I2

IP de origem	IP externo do túnel 2
Dest IP	Gateway do cliente
Protocolo	UDP
Porta de origem	500
Porta de destino	500

Regra de entrada I3

IP de origem	IP externo do túnel 1
Dest IP	Gateway do cliente
Protocolo	IP 50 (ESP)

Regra de entrada I4

IP de origem	IP externo do túnel 2
Dest IP	Gateway do cliente

Protocolo IP 50 (ESP)

Saída (para a Internet)

Regra de saída O1

IP de origem Gateway do cliente

Dest IP IP externo do túnel 1

Protocolo UDP

Porta de origem 500

Porta de destino 500

Regra de saída O2

IP de origem Gateway do cliente

Dest IP IP externo do túnel 2

Protocolo UDP

Porta de origem 500

Porta de destino 500

Regra de saída O3

IP de origem Gateway do cliente

Dest IP IP externo do túnel 1

Protocolo IP 50 (ESP)

Regra de saída O4

IP de origem Gateway do cliente

Dest IP IP externo do túnel 2

Protocolo

IP 50 (ESP)

As regras I1, I2, O1 e O2 permitem a transmissão de pacotes. IKE As regras I3, I4, O3 e O4 permitem a transmissão de IPsec pacotes que contêm o tráfego de rede criptografado.

Note

Se você estiver usando NAT traversal (NAT-T) em seu dispositivo, certifique-se de que o UDP tráfego na porta 4500 também possa passar entre sua rede e os endpoints. AWS Site-to-Site VPN Verifique se seu dispositivo está anunciando NAT -T.

Exemplos de arquivos de configuração para seu dispositivo de gateway do cliente

Depois de criar a VPN conexão, você também tem a opção de baixar um arquivo de configuração de amostra AWS fornecido no VPC console da Amazon ou usando o. EC2 API Consulte [Etapa 6: baixar o arquivo de configuração](#) Para mais informações. Você também pode baixar arquivos.zip de configurações de amostra especificamente para roteamento estático versus dinâmico a partir dessas respectivas páginas.

O arquivo AWS de configuração de amostra fornecido contém informações específicas de sua VPN conexão que você pode usar para configurar seu dispositivo de gateway do cliente. Esses arquivos de configuração específicos do dispositivo estão disponíveis somente para dispositivos que AWS foram testados. Se o dispositivo de gateway do cliente específico não estiver listado, você poderá baixar um arquivo de configuração genérica para começar.

Important

O arquivo de configuração é apenas um exemplo e pode não corresponder totalmente às configurações de VPN conexão de site a site pretendidas. Ele especifica os requisitos mínimos para uma VPN conexão site a site de AES128,, e do grupo Diffie-Hellman 2 na maioria das regiões e SHA1,, e do grupo Diffie-Hellman 14 AWS nas regiões. AES128 SHA2 AWS GovCloud Ele também especifica chaves pré-compartilhadas para autenticação. Você deve modificar o arquivo de configuração de exemplo para aproveitar os algoritmos de segurança adicionais, grupos Diffie-Hellman, certificados privados e tráfego. IPv6

Note

Esses arquivos de configuração específicos do dispositivo são fornecidos com AWS base no melhor esforço. Embora tenham sido testados por AWS, esse teste é limitado. Em caso de problemas com os arquivos de configuração, talvez seja necessário entrar em contato com o fornecedor específico para obter suporte adicional.

A tabela a seguir contém uma lista de dispositivos que têm um exemplo de arquivo de configuração disponível para download que foi atualizado para oferecer suporte IKEv2. Introduzimos IKEv2 suporte nos arquivos de configuração para muitos dispositivos populares de gateway de clientes e continuaremos adicionando arquivos adicionais com o passar do tempo. Esta lista será atualizada à medida que mais arquivos de configuração de exemplo forem adicionados.

Vendor	Plataforma	Software
Ponto de verificação	Gaia	R80.10+
Cisco Meraki	MX Series	15.12+ (WebUI)
Cisco Systems, Inc.	ASA Série 5500	ASA9,7 ou mais VTI
Cisco Systems, Inc.	CSRv AMI	IOS12,4+
Fortinet	Fortigate 40+ Series	FortiOS 6.4.4+ () GUI
Juniper Networks, Inc.	J-Series Routers	JunOS 9.5+
Juniper Networks, Inc.	SRX Roteadores	JunOS 11.0+
Mikrotik	RouterOS	6.4.3
Palo Alto Networks	PA Series	PANOS7.0+
SonicWall	NSA, TZ	OS 6.5
Sophos	Sophos Firewall	v19+
Strongswan	Ubuntu 16.04	Strongswan 5.5.1+

Vendor	Plataforma	Software
Yamaha	RTXRoteadores	Rev.10.01.16+

Exemplo de configurações de dispositivos de gateway do cliente para roteamento estático

Para baixar um arquivo de configuração de amostra com valores específicos para sua configuração de VPN conexão site a site, use o VPC console da Amazon, a linha de AWS comando ou a Amazon. EC2 API Para obter mais informações, consulte [Etapa 6: baixar o arquivo de configuração](#).

[Você também pode baixar arquivos de configuração de exemplo genéricos para roteamento estático que não incluem valores específicos para sua configuração de conexão site a site: .zip VPN static-routing-examples](#)

Os arquivos usam valores de espaço reservado para alguns componentes. Por exemplo, eles usam:

- Valores de exemplo para ID de VPN conexão, ID do gateway do cliente e ID do gateway privado virtual
- Espaços reservados para os AWS endpoints de endereço IP remotos (externos) (*AWS_ENDPOINT_1* e *AWS_ENDPOINT_2*)
- Um espaço reservado para o endereço IP da interface externa roteável pela Internet no dispositivo de gateway do cliente (*your-cgw-ip-address*)
- Um espaço reservado para o valor da chave pré-compartilhada () pre-shared-key
- Valores de exemplo para o túnel dentro de endereços IP.
- Valores de exemplo para MTU configuração.

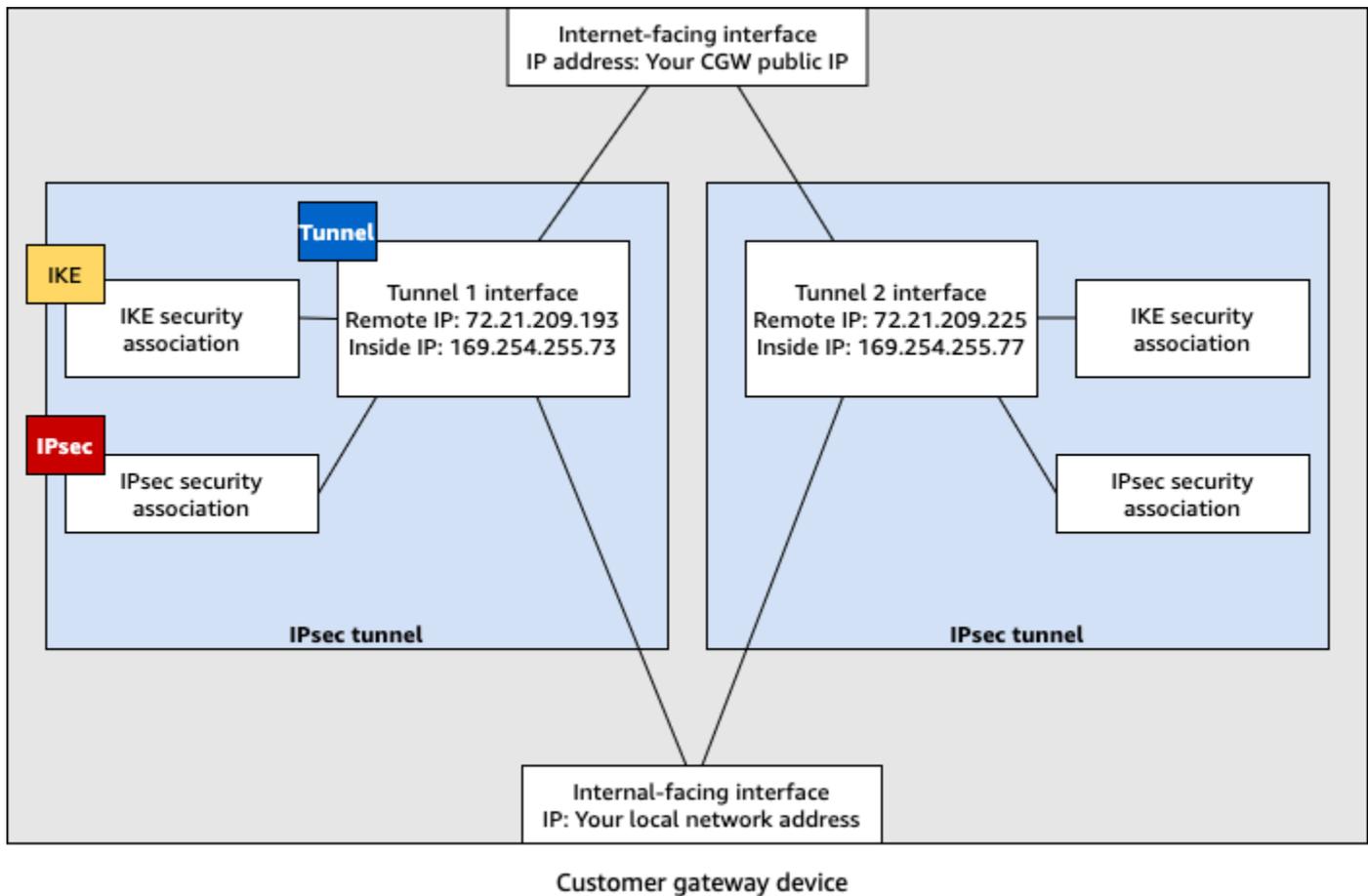
Note

MTUas configurações fornecidas nos arquivos de configuração de amostra são apenas exemplos. Consulte [Práticas recomendadas para o dispositivo de gateway do cliente](#) para obter informações sobre como definir o MTU valor ideal para sua situação.

Além de fornecer valores de espaço reservado, os arquivos especificam os requisitos mínimos para uma VPN conexão site a site deAES128,, e do grupo Diffie-Hellman 2 na maioria das regiões

eSHA1, e do grupo Diffie-Hellman 14 AWS nas regiões. AES128 SHA2 AWS GovCloud Eles também especificam chaves pré-compartilhadas para [autenticação](#). Você deve modificar o arquivo de configuração de exemplo para aproveitar os algoritmos de segurança adicionais, grupos Diffie-Hellman, certificados privados e tráfego. IPv6

O diagrama a seguir fornece uma visão geral dos diferentes componentes configurados no dispositivo de gateway do cliente. Ele inclui valores de exemplo para os endereços IP da interface do túnel.



Procedimentos da interface do usuário para roteamento estático

Veja a seguir alguns procedimentos de exemplo para configurar um dispositivo de gateway do cliente usando sua interface de usuário (se disponível).

Check Point

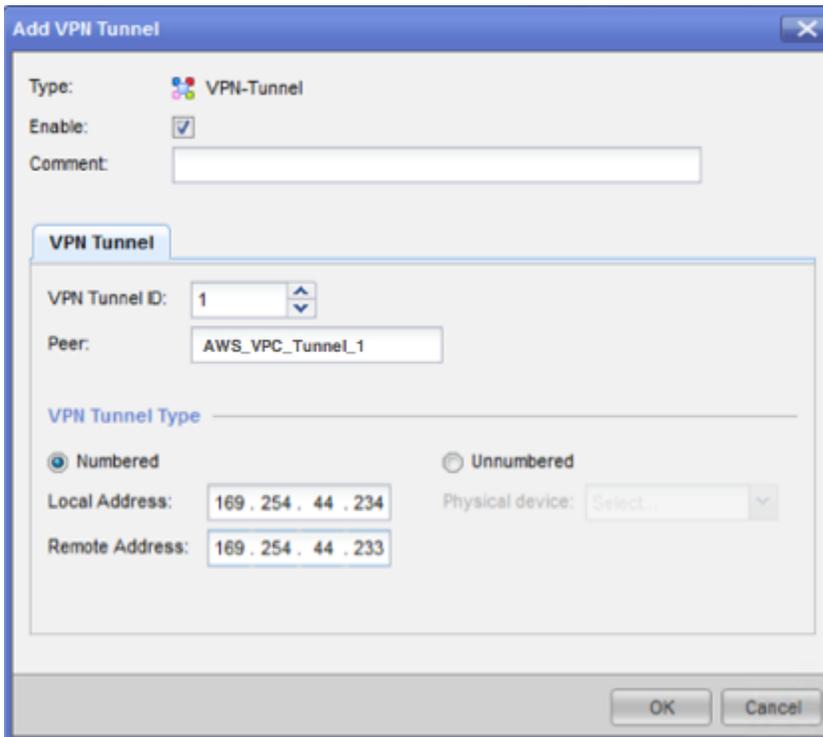
A seguir estão as etapas para configurar seu dispositivo de gateway de cliente se seu dispositivo for um dispositivo Check Point Security Gateway executando R77.10 ou superior, usando o sistema operacional Gaia e o Check Point. SmartDashboard Você também pode consultar o VPC

artigo do [Check Point Security Gateway IPsec VPN to Amazon Web Services](#) no Check Point Support Center.

Para configurar a interface do túnel

A primeira etapa é criar os VPN túneis e fornecer os endereços IP privados (internos) do gateway do cliente e do gateway privado virtual para cada túnel. Para criar o primeiro túnel, use as informações fornecidas na seção IPsec Tunnel #1 do arquivo de configuração. Para criar o segundo túnel, use os valores fornecidos na seção IPsec Tunnel #2 do arquivo de configuração.

1. Abra o portal Gaia do dispositivo Check Point Security Gateway.
2. Escolha Interfaces de rede, Adicionar, VPNtúnel.
3. Na caixa de diálogo, defina as configurações como a seguir e escolha OK ao concluir:
 - Em ID do VPN túnel, insira qualquer valor exclusivo, como 1.
 - Em Peer, insira um nome exclusivo para seu túnel, como AWS_VPC_Tunnel_1 or AWS_VPC_Tunnel_2.
 - Confirme se Numbered (Numerado) está selecionado e, em Local Address (Endereço local), insira o endereço IP especificado para CGW Tunnel IP no arquivo de configuração; por exemplo, 169.254.44.234.
 - Em Remote Address, insira o endereço IP especificado para VGW Tunnel IP no arquivo de configuração; por exemplo, 169.254.44.233.



4. Conecte-se ao seu gateway de segurança por meio deSSH. Se estiver usando um shell não padrão, mude para clish executando o comando a seguir: `clish`
5. Para o túnel 1, execute o comando a seguir:

```
set interface vpnt1 mtu 1436
```

Para o túnel 2, execute o comando a seguir:

```
set interface vpnt2 mtu 1436
```

6. Repita essas etapas para criar um segundo túnel, usando as informações na seção IPsec Tunnel #2 do arquivo de configuração.

Para configurar rotas estáticas

Nesta etapa, especifique a rota estática para a sub-rede em VPC para cada túnel para permitir que você envie tráfego pelas interfaces do túnel. O segundo túnel permite failover, caso haja um problema com o primeiro túnel. Se um problema é detectado, a rota estática baseada na política é removida da tabela de roteamento e a segunda rota é ativada. Você deve também ativar o

gateway do Check Point para executar ping na outra extremidade do túnel e verificar se o túnel está ativo.

1. No portal Gaia, escolha Rotas IPv4 estáticas, Adicionar.
2. Especifique o CIDR da sua sub-rede, por exemplo, 10.28.13.0/24.
3. Escolha Add Gateway, IP Address.
4. Insira o endereço IP especificado para VGW Tunnel IP no arquivo de configuração (por exemplo, 169.254.44.233) e especifique 1 como prioridade.
5. Selecione Ping.
6. Repita as etapas 3 e 4 para o segundo túnel, usando o valor VGW Tunnel IP na seção IPsec Tunnel #2 do arquivo de configuração. Especifique 2 como prioridade.

Destination: 10.28.13.0/24

Next Hop Type: Normal

Normal: Accept and forward packets.
Reject: Drop packets, and send unreachable messages.
Black Hole: Drop packets, but don't send unreachable messages.

Rank: Default: 60

Local Scope:

Comment:

Add Gateway

Ping:

Gateway	Priority
169.254.44.233	1
169.254.44.5	2

Save Cancel

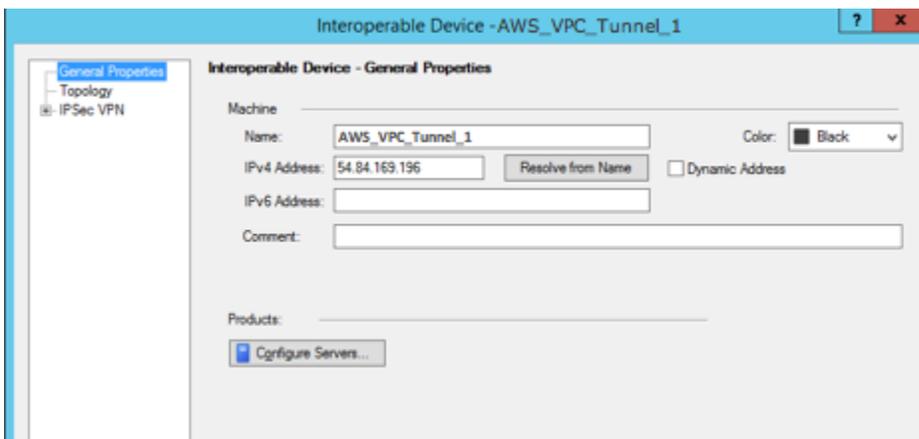
7. Escolha Salvar.

Se estiver usando um cluster, repita as etapas anteriores para os outros membros do cluster.

Para definir um novo objeto de rede

Nesta etapa, você cria um objeto de rede para cada VPN túnel, especificando os endereços IP públicos (externos) para o gateway privado virtual. Posteriormente, você adiciona esses objetos de rede como gateways de satélite para sua VPN comunidade. Você também precisa criar um grupo vazio para atuar como espaço reservado para o VPN domínio.

1. Abra o Check Point SmartDashboard.
2. Em Groups, abra o menu de contexto e escolha Groups, Simple Group. Você pode usar o mesmo grupo para cada objeto de rede.
3. Em Network Objects, abra o menu de contexto (clique com o botão direito) e escolha New, Interoperable Device.
4. Em Name (Nome), insira o nome que você forneceu para o túnel; por exemplo, AWS_VPC_Tunnel_1 ou AWS_VPC_Tunnel_2.
5. Em IPv4Endereço, insira o endereço IP externo do gateway privado virtual fornecido no arquivo de configuração, por exemplo, 54.84.169.196. Salve as configurações e feche a caixa de diálogo.



6. Em SmartDashboard, abra as propriedades do gateway e, no painel de categorias, escolha Topologia.
7. Para recuperar a configuração da interface, escolha Get Topology.
8. Na seção VPNDomínio, escolha Definido manualmente e, em seguida, procure e selecione o grupo simples vazio que você criou na etapa 2. Escolha OK.

Note

Você pode manter qualquer VPN domínio existente que tenha configurado. No entanto, certifique-se de que os hosts e as redes usados ou atendidos pela nova

VPN conexão não sejam declarados nesse VPN domínio, especialmente se o VPN domínio for derivado automaticamente.

9. Repita essas etapas para criar um segundo objeto de rede, usando as informações na seção IPsec Tunnel #2 do arquivo de configuração.

 Note

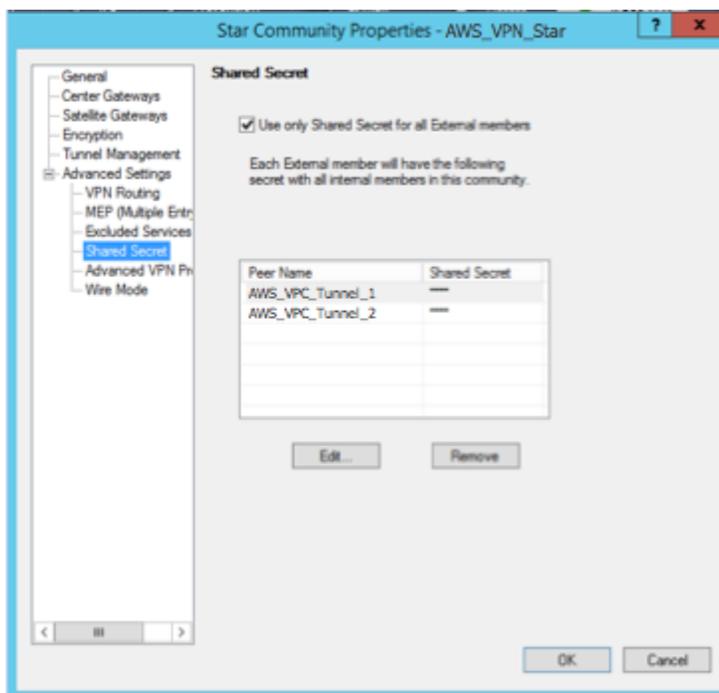
Se estiver usando clusters, edite a topologia e defina as interfaces como interfaces de cluster. Use os endereços IP especificados no arquivo de configuração.

Para criar e definir a VPN comunidade IKE e IPsec as configurações

Nesta etapa, você cria uma VPN comunidade em seu gateway Check Point, à qual adiciona os objetos de rede (dispositivos interoperáveis) para cada túnel. Você também define o Internet Key Exchange (IKE) e IPsec as configurações.

1. Nas propriedades do seu gateway, escolha IPsecVPN no painel de categorias.
2. Escolha Communities, New, Star Community.
3. Forneça um nome para a comunidade (por exemplo, AWS_VPN_Star) e escolha Center Gateways no painel de categoria.
4. Escolha Add e adicione o gateway ou cluster à lista de gateways participantes.
5. No painel de categoria, escolha Satellite Gateways (Gateways secundários), Add (Adicionar) e adicione os dispositivos interoperáveis que você criou anteriormente (AWS_VPC_Tunnel_1 e AWS_VPC_Tunnel_2) à lista de gateways participantes.
6. No painel de categoria, escolha Encryption. Na seção Método de criptografia, escolha IKEv1 somente. Na seção Encryption Suite, escolha Custom, Custom Encryption.
7. Na caixa de diálogo, configure as propriedades de criptografia como a seguir e escolha OK ao concluir:
 - IKE Propriedades da Associação de Segurança (Fase 1):
 - Execute a criptografia de troca de chaves com: AES -128
 - Execute a integridade dos dados com: SHA -1
 - IPsec Propriedades da Associação de Segurança (Fase 2):

- Execute a criptografia de IPsec dados com: AES -128
 - Execute a integridade dos dados com: SHA -1
8. No painel de categoria, escolha Tunnel Management. Escolha Set Permanent Tunnels, On all tunnels in the community. Na seção Compartilhamento de VPN túneis, escolha Um VPN túnel por par de gateway.
 9. No painel de categoria, expanda Advanced Settings e escolha Shared Secret.
 10. Selecione o nome do par do primeiro túnel, escolha Edit (Editar) e insira a chave pré-compartilhada conforme especificado no arquivo de configuração na seção IPsec Tunnel #1.
 11. Selecione o nome do par do segundo túnel, escolha Edit (Editar) e insira a chave pré-compartilhada conforme especificado no arquivo de configuração na seção IPsec Tunnel #2.



12. Ainda na categoria Configurações avançadas, escolha VPNPropriedades avançadas, configure as propriedades da seguinte forma e escolha OK quando terminar:
 - IKE(Fase 1):
 - Use Diffie-Hellman group (Usar grupo Diffie-Hellman): Group 2
 - Renegocie associações de IKE segurança a cada minuto **480**
 - IPsec(Fase 2):
 - Escolha Use Perfect Forward Secrecy

- Use Diffie-Hellman group (Usar grupo Diffie-Hellman): Group 2
- Renegocie associações de IPsec segurança a cada segundo **3600**

Para criar regras de firewall

Nesta etapa, você configura uma política com regras de firewall e regras de correspondência direcional que permitem a comunicação entre a rede VPC e a rede local. Em seguida, você instalará a política em seu gateway.

1. No SmartDashboard, escolha Propriedades globais para seu gateway. No painel de categorias VPN, expanda e escolha Avançado.
2. Escolha Ativar correspondência VPN direcional na VPN coluna e salve suas alterações.
3. No SmartDashboard, escolha Firewall e crie uma política com as seguintes regras:
 - Permita que a VPC sub-rede se comunique com a rede local por meio dos protocolos necessários.
 - Permita que a rede local se comunique com a VPC sub-rede pelos protocolos necessários.
4. Abra o menu de contexto da célula na VPN coluna e escolha Editar célula.
5. Na VPN caixa de diálogo Condições de correspondência, escolha Combinar tráfego somente nessa direção. Crie as regras de correspondência direcional a seguir escolhendo Add para cada uma e escolha OK ao concluir:
 - `internal_clear > VPN comunidade` (a comunidade VPN estrela que você criou anteriormente, por exemplo `AWS_VPN_Star`)
 - `VPN comunidade > VPN comunidade`
 - `VPN comunidade > internal_clear`
6. Em SmartDashboard, escolha Política, Instalar.
7. Na caixa de diálogo, escolha seu gateway e clique em OK para instalar a política.

Para modificar a propriedade `tunnel_keepalive_method`

Seu gateway Check Point pode usar Dead Peer Detection (DPD) para identificar quando uma IKE associação está inativa. DPDP para configurar um túnel permanente, o túnel permanente deve ser configurado na AWS VPN comunidade (consulte a Etapa 8).

Por padrão, a `tunnel_keepalive_method` propriedade de um VPN gateway é definida como `tunnel_test`. Você precisa alterar o valor para `dpd`. Cada VPN gateway na VPN comunidade que requer DPD monitoramento deve ser configurado com a `tunnel_keepalive_method` propriedade, incluindo qualquer VPN gateway de terceiros. Você não pode configurar diferentes mecanismos de monitoramento para o mesmo gateway.

Você pode atualizar a `tunnel_keepalive_method` propriedade usando a `uiDBedit` ferramenta G.

1. Abra o Check Point SmartDashboard e escolha Security Management Server, Domain Management Server.
2. Escolha File, Database Revision Control... e crie um snapshot de revisão.
3. Feche todas as SmartConsole janelas, como, por exemplo SmartDashboard, o SmartView Rastreador e o SmartView Monitor.
4. Inicie a `uiDBedit` ferramenta G. Para obter mais informações, consulte o artigo [Check Point Database Tool](#) no Check Point Support Center.
5. Escolha Security Management Server, Domain Management Server.
6. No painel superior esquerdo, escolha Table, Network Objects, `network_objects`.
7. No painel superior direito, selecione o objeto Security Gateway, Cluster pertinente.
8. Pressione CTRL +F ou use o menu Pesquisar para pesquisar o seguinte: `tunnel_keepalive_method`.
9. No painel inferior, abra o menu de contexto para `tunnel_keepalive_method` e escolha Edit... (Editar). Escolha `dpd` e OK.
10. Repita as etapas de 7 a 9 para cada gateway que faz parte da AWS VPN comunidade.
11. Escolha File, Save All.
12. Feche a `uiDBedit` ferramenta G.
13. Abra o Check Point SmartDashboard e escolha Security Management Server, Domain Management Server.
14. Instale a política no objeto Security Gateway, Cluster pertinente.

Para obter mais informações, consulte o artigo [Novos VPN recursos do R77.10](#) no Check Point Support Center.

Para ativar a TCP MSS fixação

TCPMSSa fixação reduz o tamanho máximo do segmento dos TCP pacotes para evitar a fragmentação do pacote.

1. Navegue até o seguinte diretório C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\.
2. Abra o Check Point Database Tool executando o arquivo GuidBEdit.exe.
3. Escolha Table, Global Properties, properties.
4. Em fw_clamp_tcp_mss, escolha Edit. Altere o valor para true e escolha OK.

Como verificar o status do túnel

Você pode verificar o status do túnel executando o comando a seguir na ferramenta da linha de comando, no modo especialista.

```
vpn tunnelutil
```

Nas opções exibidas, escolha 1 para verificar as IKE associações e 2 para verificar as IPsec associações.

Você pode usar também Check Point Smart Tracker Log para verificar se os pacotes na conexão estão sendo criptografados. Por exemplo, o registro a seguir indica que um pacote para o VPC foi enviado pelo túnel 1 e foi criptografado.

Log Info		Rule	
Product	Security Gateway/Management	Action	Encrypt
Date	4Nov2015	Rule	4
Time	9:42:01	Current Rule Number	4-Standard
Number	21254	Rule Name	---
Type	Log	User	---
Origin	cpgw-997695	More	
Traffic		Rule UID	{0AA18015-FF7B-4650-B0CE-3989E658CF04}
Source	Management_PC (192.168.1.116)	Community	AWS_VPN_Star
Destination	10.28.13.28	Encryption Scheme	IKE
Service	---	Data Encryption Methods	ESP: AES-128 + SHA1 + PFS (group 2)
Protocol	icmp	VPN Peer Gateway	AWS_VPC_Tunnel_1 (54.84.169.196)
Interface	eth0	Subproduct	VPN
Source Port	---	VPN Feature	VPN
Policy		Product Family	Network
Policy Name	Standard	Information	service_id: icmp-proto ICMP: Echo Request ICMP Type: 8 ICMP Code: 0
Policy Date	Tue Nov 03 11:33:45 2015		
Policy Management	cpgw-997695		

SonicWALL

O procedimento a seguir demonstra como configurar os VPN túneis no dispositivo Sonic WALL usando a interface de gerenciamento do SonicOS.

Para configurar os túneis

1. Abra a interface de gerenciamento do Sonic WALL SonicOS.
2. No painel esquerdo VPN, escolha Configurações. Em VPNPolíticas, escolha Adicionar... .
3. Na janela VPN de política na guia Geral, preencha as seguintes informações:
 - Policy Type (Tipo de política): escolha Tunnel Interface (Interface do túnel).
 - Método de autenticação: escolha IKEusando o segredo pré-compartilhado.
 - Nome: insira um nome para a VPN política. Recomendamos que você use o nome do VPN ID, conforme fornecido no arquivo de configuração.
 - IPsecNome ou endereço do gateway primário: insira o endereço IP do gateway privado virtual conforme fornecido no arquivo de configuração (por exemplo,72 . 21 . 209 . 193).
 - IPsecNome ou endereço do gateway secundário: deixe o valor padrão.

- Shared Secret: Insira a chave pré-compartilhada conforme fornecida no arquivo de configuração, e insira-a novamente em Confirm Shared Secret.
 - IKEID local: insira o IPv4 endereço do gateway do cliente (o WALL dispositivo Sonic).
 - IKEID do peer: insira o IPv4 endereço do gateway privado virtual.
4. Na guia Network, conclua com as seguintes informações:
- Em Local Networks, escolha Any address. Recomendamos esta opção para evitar problemas de conectividade na rede local.
 - Em Remote Networks, escolha Choose a destination network from list. Crie um objeto de endereço com o CIDR de sua VPC entrada AWS.
5. Na guia Proposals (Propostas) conclua com as seguintes informações.
- Em Proposta IKE (Fase 1), faça o seguinte:
 - Exchange: Escolha Main Mode.
 - DH Group (Grupo DH): insira um valor para o grupo Diffie-Hellman (por exemplo, 2).
 - Criptografia: escolha AES-128 ou AES-256.
 - Autenticação: escolha SHA1 ou SHA256.
 - Life Time: Insira 28800.
 - Em Proposta IKE (Fase 2), faça o seguinte:
 - Protocolo: Escolha ESP.
 - Criptografia: escolha AES-128 ou AES-256.
 - Autenticação: escolha SHA1 ou SHA256.
 - Selecione a caixa de seleção Enable Perfect Forward Secrecy e escolha o grupo Diffie-Hellman.
 - Life Time: Insira 3600.

 Important

Se você criou seu gateway privado virtual antes de outubro de 2015, você deve especificar o grupo Diffie-Hellman 2, AES -128 e para ambas as fases. SHA1

6. Na guia Advanced conclua com as seguintes informações:

- Selecione Enable Keep Alive

- Selecione Enable Phase2 Dead Peer Detection e insira o seguinte:
 - Para Dead Peer Detection Interval, digite 60 (esse é o mínimo que o WALL dispositivo Sonic aceita).
 - Em Failure Trigger Level, insira 3.
 - Em VPNPolítica vinculada a, selecione Interface X1. Essa é a interface designada normalmente para endereços IP públicos.
- 7. Escolha OK. Na página Configurações a caixa de seleção Habilitar para o túnel deve ser selecionada por padrão. Um ponto verde indica que o túnel está ativo.

Informações adicionais para dispositivos Cisco

Alguns Cisco suportam ASAs apenas o modo ativo/em espera. Quando você usa esses CiscoASAs, você pode ter somente um túnel ativo por vez. O outro túnel em espera ficará ativo se o primeiro túnel ficar indisponível. Com essa redundância, você deve sempre ter conectividade com você VPC por meio de um dos túneis.

A Cisco ASAs da versão 9.7.1 e posterior suporta o modo ativo/ativo. Ao usar esses CiscoASAs, você pode ter os dois túneis ativos ao mesmo tempo. Com essa redundância, você deve sempre ter conectividade com você VPC por meio de um dos túneis.

Para dispositivos Cisco, é necessário fazer o seguinte:

- Configurar a interface externa.
- Certifique-se de que o número ISAKMP de sequência da política de criptografia seja exclusivo.
- Garanta que o número Crypto List Policy Sequence seja exclusivo.
- Certifique-se de que o Crypto IPsec Transform Set e a Crypto ISAKMP Policy Sequence estejam em harmonia com quaisquer outros IPsec túneis configurados no dispositivo.
- Certifique-se de que o número de SLA monitoramento seja exclusivo.
- Configurar todo o roteamento interno que move o tráfego entre o gateway do cliente e a rede local.

Exemplo de configurações de dispositivos de gateway do cliente para roteamento dinâmico

Para baixar um arquivo de configuração de amostra com valores específicos para sua configuração de VPN conexão site a site, use o VPC console da Amazon, a linha de AWS comando ou a Amazon EC2 API. Para obter mais informações, consulte [Etapa 6: baixar o arquivo de configuração](#).

[Você também pode baixar arquivos de configuração de exemplo genéricos para roteamento dinâmico que não incluem valores específicos para sua configuração de conexão site a site: .zip VPN dynamic-routing-examples](#)

Os arquivos usam valores de espaço reservado para alguns componentes. Por exemplo, eles usam:

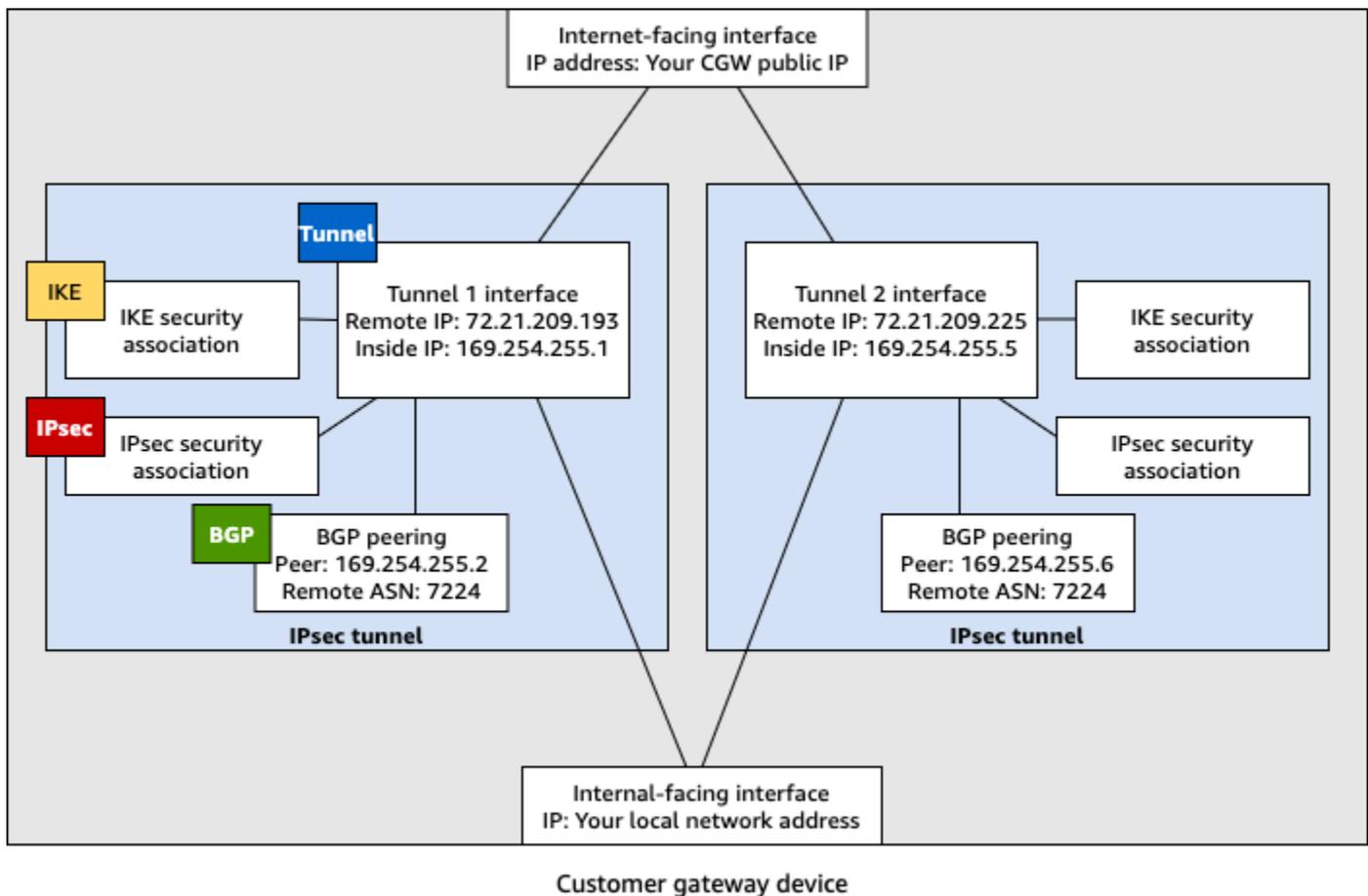
- Valores de exemplo para a ID da VPN conexão, ID do gateway do cliente e ID do gateway privado virtual
- Espaços reservados para os AWS endpoints de endereço IP remotos (externos) (*AWS_ENDPOINT_1* e *AWS_ENDPOINT_2*)
- Um espaço reservado para o endereço IP da interface externa roteável pela Internet no dispositivo de gateway do cliente (*your-cgw-ip-address*)
- Um espaço reservado para o valor da chave pré-compartilhada () pre-shared-key
- Valores de exemplo para o túnel dentro de endereços IP.
- Valores de exemplo para MTU configuração.

Note

MTUAs configurações fornecidas nos arquivos de configuração de amostra são apenas exemplos. Consulte [Práticas recomendadas para o dispositivo de gateway do cliente](#) para obter informações sobre como definir o MTU valor ideal para sua situação.

Além de fornecer valores de espaço reservado, os arquivos especificam os requisitos mínimos para uma VPN conexão site a site de AES128,, e do grupo Diffie-Hellman 2 na maioria das regiões e SHA1, e do grupo Diffie-Hellman 14 AWS nas regiões. AES128 SHA2 AWS GovCloud Eles também especificam chaves pré-compartilhadas para [autenticação](#). Você deve modificar o arquivo de configuração de exemplo para aproveitar os algoritmos de segurança adicionais, grupos Diffie-Hellman, certificados privados e tráfego. IPv6

O diagrama a seguir fornece uma visão geral dos diferentes componentes configurados no dispositivo de gateway do cliente. Ele inclui valores de exemplo para os endereços IP da interface do túnel.



Procedimentos da interface do usuário para roteamento dinâmico

Veja a seguir alguns procedimentos de exemplo para configurar um dispositivo de gateway do cliente usando sua interface de usuário (se disponível).

Check Point

A seguir estão as etapas para configurar um dispositivo Check Point Security Gateway executando o R77.10 ou superior, usando o portal web Gaia e o Check Point. SmartDashboard. Você também pode consultar o VPN BGP artigo [da Amazon Web Services \(AWS\)](#) no Check Point Support Center.

Para configurar a interface do túnel

A primeira etapa é criar os VPN túneis e fornecer os endereços IP privados (internos) do gateway do cliente e do gateway privado virtual para cada túnel. Para criar o primeiro túnel, use as informações fornecidas na seção `IPSec Tunnel #1` do arquivo de configuração. Para criar o segundo túnel, use os valores fornecidos na seção `IPSec Tunnel #2` do arquivo de configuração.

1. Conecte-se ao seu gateway de segurança por meio de SSH. Se estiver usando um shell não padrão, mude para `clish` executando o comando a seguir: `clish`
2. Defina o gateway do cliente ASN (o ASN que foi fornecido quando o gateway do cliente foi criado em AWS) executando o comando a seguir.

```
set as 65000
```

3. Crie a interface para o primeiro túnel, usando as informações fornecidas na seção `IPSec Tunnel #1` do arquivo de configuração. Forneça um nome exclusivo para seu túnel, como `AWS_VPC_Tunnel_1`.

```
add vpn tunnel 1 type numbered local 169.254.44.234 remote 169.254.44.233  
peer AWS_VPC_Tunnel_1  
set interface vpnt1 state on  
set interface vpnt1 mtu 1436
```

4. Repita esses comandos para criar o segundo túnel, usando as informações fornecidas na seção `IPSec Tunnel #2` do arquivo de configuração. Forneça um nome exclusivo para seu túnel, como `AWS_VPC_Tunnel_2`.

```
add vpn tunnel 1 type numbered local 169.254.44.38 remote 169.254.44.37  
peer AWS_VPC_Tunnel_2  
set interface vpnt2 state on  
set interface vpnt2 mtu 1436
```

5. Defina o gateway privado virtual ASN.

```
set bgp external remote-as 7224 on
```

6. Configure o BGP para o primeiro túnel, usando a `IPSec Tunnel #1` seção de informações fornecidas do arquivo de configuração.

```
set bgp external remote-as 7224 peer 169.254.44.233 on
set bgp external remote-as 7224 peer 169.254.44.233 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.233 keepalive 10
```

7. Configure o BGP para o segundo túnel, usando a IPsec Tunnel #2 seção de informações fornecidas do arquivo de configuração.

```
set bgp external remote-as 7224 peer 169.254.44.37 on
set bgp external remote-as 7224 peer 169.254.44.37 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.37 keepalive 10
```

8. Salve a configuração.

```
save config
```

Para criar uma BGP política

Em seguida, crie uma BGP política que permita a importação de rotas anunciadas por AWS. Em seguida, configure seu gateway do cliente para anunciar suas rotas locais para a AWS.

1. Na Gaia WebUI, escolha Advanced Routing, Inbound Route Filters. Escolha Adicionar e selecione Adicionar BGP política (com base no AS).
2. Em Adicionar BGP política, selecione um valor entre 512 e 1024 no primeiro campo e insira o gateway privado virtual ASN no segundo campo (por exemplo, 7224).
3. Escolha Salvar.

Para anunciar rotas locais

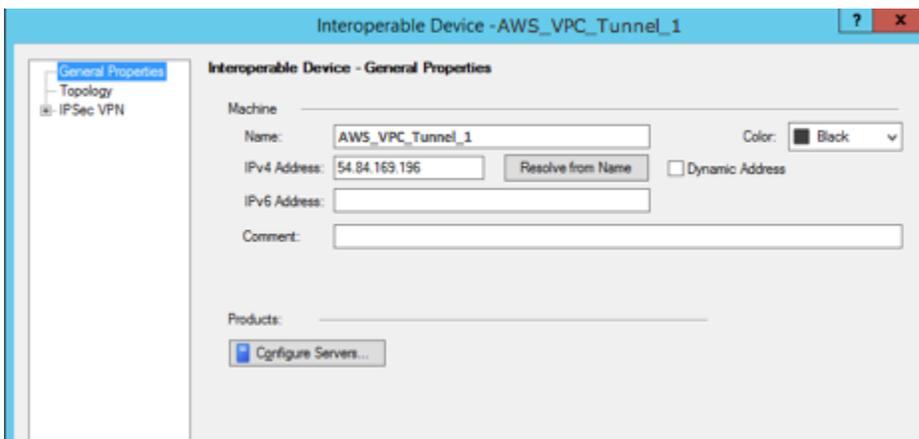
As etapas a seguir destinam-se à distribuição de rotas de interface locais. Além disso, você pode redistribuir as rotas de diferentes origens (por exemplo, rotas estáticas ou rotas obtidas por meio de protocolos de roteamento dinâmico). Para obter mais informações, consulte [Gaia Advanced Routing R77 Versions Administration Guide](#).

1. Na Gaia WebUI, escolha Advanced Routing, Routing Redistribution. Selecione Add Redistribution From (Adicionar redistribuição de) e escolha Interface.
2. Em Para Protocolo, selecione o gateway privado virtual ASN (por exemplo, 7224).
3. Em Interface, selecione uma interface interna. Escolha Salvar.

Para definir um novo objeto de rede

Em seguida, crie um objeto de rede para cada VPN túnel, especificando os endereços IP públicos (externos) para o gateway privado virtual. Posteriormente, você adiciona esses objetos de rede como gateways de satélite para sua VPN comunidade. Você também precisa criar um grupo vazio para atuar como espaço reservado para o VPN domínio.

1. Abra o Check Point SmartDashboard.
2. Em Groups, abra o menu de contexto e escolha Groups, Simple Group. Você pode usar o mesmo grupo para cada objeto de rede.
3. Em Network Objects, abra o menu de contexto (clique com o botão direito) e escolha New, Interoperable Device.
4. Em Name (Nome), insira o nome que você forneceu para o túnel na etapa 1, por exemplo, AWS_VPC_Tunnel_1 ou AWS_VPC_Tunnel_2.
5. Em IPv4Endereço, insira o endereço IP externo do gateway privado virtual fornecido no arquivo de configuração, por exemplo, 54.84.169.196. Salve as configurações e feche a caixa de diálogo.



6. No painel de categoria, escolha Topology.
7. Na seção VPNDomínio, escolha Definido manualmente e, em seguida, procure e selecione o grupo simples vazio que você criou na etapa 2. Escolha OK.
8. Repita essas etapas para criar um segundo objeto de rede, usando as informações na seção IPSec Tunnel #2 do arquivo de configuração.
9. Acesse o objeto de rede do gateway, abra o gateway ou objeto do cluster e escolha Topology.
10. Na seção VPNDomínio, escolha Definido manualmente e, em seguida, procure e selecione o grupo simples vazio que você criou na etapa 2. Escolha OK.

Note

Você pode manter qualquer VPN domínio existente que tenha configurado. No entanto, certifique-se de que os hosts e as redes usados ou atendidos pela nova VPN conexão não sejam declarados nesse VPN domínio, especialmente se o VPN domínio for derivado automaticamente.

Note

Se estiver usando clusters, edite a topologia e defina as interfaces como interfaces de cluster. Use os endereços IP especificados no arquivo de configuração.

Para criar e definir a VPN comunidade IKE e IPsec as configurações

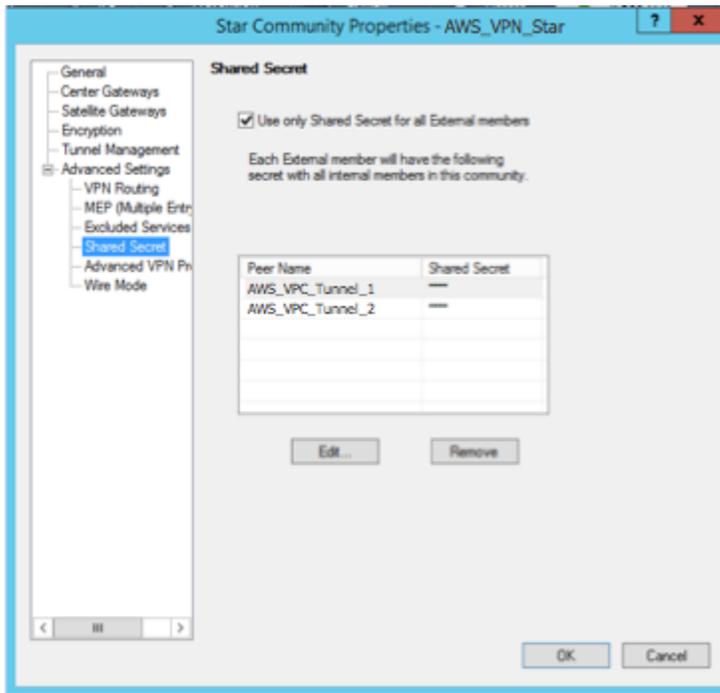
Em seguida, crie uma VPN comunidade em seu gateway Check Point, à qual você adiciona os objetos de rede (dispositivos interoperáveis) para cada túnel. Você também define o Internet Key Exchange (IKE) e IPsec as configurações.

1. Nas propriedades do seu gateway, escolha IPsecVPN no painel de categorias.
2. Escolha Communities, New, Star Community.
3. Forneça um nome para a comunidade (por exemplo, AWS_VPN_Star) e escolha Center Gateways no painel de categoria.
4. Escolha Add e adicione o gateway ou cluster à lista de gateways participantes.
5. No painel de categoria, selecione Satellite Gateways (Gateways secundários), Add (Adicionar) e adicione os dispositivos interoperáveis criados anteriormente (AWS_VPC_Tunnel_1 e AWS_VPC_Tunnel_2) à lista de gateways participantes.
6. No painel de categoria, escolha Encryption. Na seção Método de criptografia, escolha IKEv1 para IPv4 e IKEv2 para IPv6. Na seção Encryption Suite, escolha Custom, Custom Encryption.

Note

Você deve selecionar a IPv6 opção IKEv1 para IPv4 e IKEv2 para para a IKEv1 funcionalidade.

7. Na caixa de diálogo, configure as propriedades de criptografia como indicado a seguir e selecione OK ao concluir:
 - IKEPropriedades da Associação de Segurança (Fase 1):
 - Execute a criptografia de troca de chaves com: AES -128
 - Execute a integridade dos dados com: SHA -1
 - IPsecPropriedades da Associação de Segurança (Fase 2):
 - Execute a criptografia de IPsec dados com: AES -128
 - Execute a integridade dos dados com: SHA -1
8. No painel de categoria, escolha Tunnel Management. Escolha Set Permanent Tunnels, On all tunnels in the community. Na seção Compartilhamento de VPN túneis, escolha Um VPN túnel por par de gateway.
9. No painel de categoria, expanda Advanced Settings e escolha Shared Secret.
10. Selecione o nome do par do primeiro túnel, escolha Edit (Editar) e insira a chave pré-compartilhada conforme especificado no arquivo de configuração na seção IPsec Tunnel #1.
11. Selecione o nome do par do segundo túnel, escolha Edit (Editar) e insira a chave pré-compartilhada conforme especificado no arquivo de configuração na seção IPsec Tunnel #2.



12. Ainda na categoria Configurações avançadas, escolha VPNPropriedades avançadas, configure as propriedades da seguinte forma e escolha OK quando terminar:

- IKE(Fase 1):
 - Use Diffie-Hellman group (Usar grupo Diffie-Hellman): Group 2 (1024 bit)
 - Renegocie associações de IKE segurança a cada minuto **480**
- IPsec(Fase 2):
 - Escolha Use Perfect Forward Secrecy
 - Use Diffie-Hellman group (Usar grupo Diffie-Hellman): Group 2 (1024 bit)
 - Renegocie associações de IPsec segurança a cada segundo **3600**

Para criar regras de firewall

Em seguida, configure uma política com regras de firewall e regras de correspondência direcional que permitam a comunicação entre a rede VPC e a rede local. Em seguida, você instalará a política em seu gateway.

1. No SmartDashboard, escolha Propriedades globais para seu gateway. No painel de categorias VPN, expanda e escolha Avançado.
2. Escolha Ativar correspondência VPN direcional na VPN coluna e escolha OK.

3. No SmartDashboard, escolha Firewall e crie uma política com as seguintes regras:
 - Permita que a VPC sub-rede se comunique com a rede local por meio dos protocolos necessários.
 - Permita que a rede local se comunique com a VPC sub-rede pelos protocolos necessários.
4. Abra o menu de contexto da célula na VPN coluna e escolha Editar célula.
5. Na VPN caixa de diálogo Condições de correspondência, escolha Combinar tráfego somente nessa direção. Crie as regras de correspondência direcional a seguir selecionando Add (Adicionar) para cada uma e selecione OK ao concluir:
 - `internal_clear > VPN comunidade` (a comunidade VPN estrela que você criou anteriormente, por exemplo `AWS_VPN_Star`)
 - `VPN comunidade > VPN comunidade`
 - `VPN comunidade > internal_clear`
6. Em SmartDashboard, escolha Política, Instalar.
7. Na caixa de diálogo, escolha seu gateway e clique em OK para instalar a política.

Para modificar a propriedade `tunnel_keepalive_method`

Seu gateway Check Point pode usar Dead Peer Detection (DPD) para identificar quando uma IKE associação está inativa. DPDP para configurar um túnel permanente, o túnel permanente deve ser configurado na AWS VPN comunidade.

Por padrão, a `tunnel_keepalive_method` propriedade de um VPN gateway é definida como `tunnel_test`. Você precisa alterar o valor para `dpd`. Cada VPN gateway na VPN comunidade que requer DPD monitoramento deve ser configurado com a `tunnel_keepalive_method` propriedade, incluindo qualquer VPN gateway de terceiros. Você não pode configurar diferentes mecanismos de monitoramento para o mesmo gateway.

Você pode atualizar a `tunnel_keepalive_method` propriedade usando a `uiDBedit` ferramenta G.

1. Abra o Check Point SmartDashboard e escolha Security Management Server, Domain Management Server.
2. Escolha File, Database Revision Control... e crie um snapshot de revisão.
3. Feche todas as SmartConsole janelas, como, por exemplo SmartDashboard, o SmartView Rastreador e o SmartView Monitor.

4. Inicie a uiDBedit ferramenta G. Para obter mais informações, consulte o artigo [Check Point Database Tool](#) no Check Point Support Center.
5. Escolha Security Management Server, Domain Management Server.
6. No painel superior esquerdo, escolha Table, Network Objects, network_objects.
7. No painel superior direito, selecione o objeto Security Gateway, Cluster pertinente.
8. Pressione CTRL +F ou use o menu Pesquisar para pesquisar o seguinte:tunnel_keepalive_method.
9. No painel inferior, abra o menu de contexto para tunnel_keepalive_method e selecione Edit.... Escolha dpd, OK.
10. Repita as etapas de 7 a 9 para cada gateway que faz parte da AWS VPN comunidade.
11. Escolha File, Save All.
12. Feche a uiDBedit ferramenta G.
13. Abra o Check Point SmartDashboard e escolha Security Management Server, Domain Management Server.
14. Instale a política no objeto Security Gateway, Cluster pertinente.

Para obter mais informações, consulte o artigo [Novos VPN recursos do R77.10](#) no Check Point Support Center.

Para ativar a TCP MSS fixação

TCPMSSa fixação reduz o tamanho máximo do segmento dos TCP pacotes para evitar a fragmentação do pacote.

1. Navegue até o seguinte diretório C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\.
2. Abra o Check Point Database Tool executando o arquivo GuidBEdit.exe.
3. Escolha Table, Global Properties, properties.
4. Em fw_clamp_tcp_mss, escolha Edit. Altere o valor para true e selecione OK.

Como verificar o status do túnel

Você pode verificar o status do túnel executando o comando a seguir na ferramenta da linha de comando, no modo especialista.

vpn tunnelutil

Nas opções exibidas, escolha 1 para verificar as IKE associações e 2 para verificar as IPsec associações.

Você pode usar também Check Point Smart Tracker Log para verificar se os pacotes na conexão estão sendo criptografados. Por exemplo, o registro a seguir indica que um pacote para o VPC foi enviado pelo túnel 1 e foi criptografado.

Log Info		Rule	
Product	Security Gateway/Management	Action	Encrypt
Date	4Nov2015	Rule	4
Time	9:42:01	Current Rule Number	4-Standard
Number	21254	Rule Name	---
Type	Log	User	---
Origin	cpgw-997695	More	
Traffic		Rule UID	{0AA18015-FF7B-4650-B0CE-3989E658CF04}
Source	Management_PC (192.168.1.116)	Community	AWS_VPN_Star
Destination	10.28.13.28	Encryption Scheme	IKE
Service	---	Data Encryption Methods	ESP: AES-128 + SHA1 + PFS (group 2)
Protocol	icmp	VPN Peer Gateway	AWS_VPC_Tunnel_1 (54.84.169.196)
Interface	eth0	Subproduct	VPN
Source Port	---	VPN Feature	VPN
Policy		Product Family	Network
Policy Name	Standard	Information	service_id: icmp-proto ICMP: Echo Request ICMP Type: 8 ICMP Code: 0
Policy Date	Tue Nov 03 11:33:45 2015		
Policy Management	cpgw-997695		

SonicWALL

Você pode configurar um WALL dispositivo Sonic usando a interface de gerenciamento do SonicOS. Para obter mais informações sobre a configuração de túneis, consulte [Procedimentos da interface do usuário para roteamento estático](#).

Você não pode configurar BGP o dispositivo usando a interface de gerenciamento. Em vez disso, use as instruções da linha de comando fornecidas no arquivo de configuração de exemplo, na seção chamada BGP.

Informações adicionais para dispositivos Cisco

Alguns Cisco suportam ASAs apenas o modo ativo/em espera. Quando você usa esses CiscoASAs, você pode ter somente um túnel ativo por vez. O outro túnel em espera ficará ativo se o primeiro túnel ficar indisponível. Com essa redundância, você deve sempre ter conectividade com você VPC por meio de um dos túneis.

A Cisco ASAs da versão 9.7.1 e posterior suporta o modo ativo/ativo. Ao usar esses CiscoASAs, você pode ter os dois túneis ativos ao mesmo tempo. Com essa redundância, você deve sempre ter conectividade com você VPC por meio de um dos túneis.

Para dispositivos Cisco, é necessário fazer o seguinte:

- Configurar a interface externa.
- Certifique-se de que o número ISAKMP de sequência da política de criptografia seja exclusivo.
- Garanta que o número Crypto List Policy Sequence seja exclusivo.
- Certifique-se de que o Crypto IPsec Transform Set e a Crypto ISAKMP Policy Sequence estejam em harmonia com quaisquer outros IPsec túneis configurados no dispositivo.
- Certifique-se de que o número de SLA monitoramento seja exclusivo.
- Configurar todo o roteamento interno que move o tráfego entre o gateway do cliente e a rede local.

Informações adicionais para dispositivos Juniper

As informações a seguir se aplicam aos exemplos de arquivos de configuração para dispositivos Juniper J-Series e de gateway SRX do cliente.

- A interface externa é chamada de *ge-0/0/0.0*.
- A interface do IDs túnel é chamada de *st0.1* e *st0.2*.
- Certifique-se de identificar a zona de segurança da interface de uplink (as informações de configuração usam a zona padrão "untrust").
- Certifique-se de identificar a zona de segurança da interface interna (as informações de configuração usam a zona padrão "trust").

Configurar o Windows Server como um dispositivo de gateway do cliente

Você pode configurar o servidor que executa o Windows Server como um dispositivo de gateway do cliente para sua VPC. Use o processo a seguir se estiver executando o Windows Server em uma instância do EC2, em uma VPC ou em seu próprio servidor. Os procedimentos a seguir se aplicam ao Windows Server 2012 R2 e versões posteriores.

Conteúdo

- [Configurar a instância do Windows](#)
- [Etapa 1: Criar uma conexão VPN e configurar a VPC](#)
- [Etapa 2: Fazer download do arquivo de configuração para a conexão VPN](#)
- [Etapa 3: configurar o Windows Server](#)
- [Etapa 4: Configurar o túnel VPN](#)
- [Etapa 5: Habilitar a detecção de gateway inativo](#)
- [Etapa 6: Testar a conexão VPN](#)

Configurar a instância do Windows

Se você estiver configurando o Windows Server em uma instância do EC2 executada em uma AMI do Windows, faça o seguinte:

- Desative a verificação de origem/destino da instância:
 1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
 2. Selecione a sua instância do Windows e escolha Actions (Ações), Networking (Rede), Change source/destination check (Alterar verificação de origem/destino). Escolha Stop (Interromper) e, em seguida, escolha Save (Salvar).
- Atualize as configurações do adaptador de modo que você possa rotear tráfego de outras instâncias:
 1. Conecte-se à sua instância do Windows. Para obter mais informações, consulte [Conectar-se à sua instância do Windows](#).
 2. Abra o Painel de controle e inicie o Gerenciador de dispositivos.
 3. Expanda o nó Adaptadores de rede.

4. Selecione o adaptador de rede (dependendo do tipo de instância, pode ser Amazon Elastic Network Adapter ou Intel 82599 Virtual Function) e escolha Action (Ação), Properties (Propriedades).
 5. Na guia Advanced, desative as propriedades IPv4 Checksum Offload, TCP Checksum Offload (IPv4) e UDP Checksum Offload (IPv4) e escolha OK.
- Aloque um endereço IP elástico à sua conta e associe-o à instância. Para obter mais informações, consulte [Trabalhar com endereços IP elásticos](#). Anote este endereço; ele será necessário quando você criar o gateway do cliente na sua VPC.
 - Verifique se as regras do grupo de segurança da instância permitem tráfego IPsec de saída. Por padrão, um grupo de segurança permite todo o tráfego de saída. No entanto, se as regras de saída do grupo de segurança tiverem sido modificadas em relação ao seu estado original, crie as seguintes regras personalizadas de protocolo de saída para o tráfego IPsec: protocolo IP 50, protocolo IP 51 e UDP 500.

Tome nota do intervalo CIDR da rede na qual sua instância do Windows está localizada, por exemplo, 172.31.0.0/16.

Etapa 1: Criar uma conexão VPN e configurar a VPC

Para criar uma conexão VPN partindo de sua VPC, faça o seguinte:

1. Crie um gateway privado virtual e anexe-o à sua VPC. Para ter mais informações, consulte [Criar um gateway privado virtual](#).
2. Crie uma conexão VPN e um novo gateway do cliente. Para o gateway do cliente, especifique o endereço IP público do Windows Server. Para a conexão VPN, escolha roteamento estático e insira o intervalo CIDR para a rede na qual o Windows Server está localizado, por exemplo, 172.31.0.0/16. Para ter mais informações, consulte [Etapa 5: criar uma conexão VPN](#).

Depois de criar a conexão VPN, configure a VPC para habilitar a comunicação pela conexão VPN.

Para configurar a VPC

- Crie uma sub-rede privada na sua VPC (se ainda não tiver uma) para executar instâncias que se comunicarão com o Windows Server. Para obter mais informações, consulte [Criar uma sub-rede na sua VPC](#).

Note

Uma sub-rede privada é uma sub-rede que não tem uma rota para um gateway da Internet. O roteamento para esta sub-rede é descrito no próximo item.

- Atualize as tabelas de rotas para a conexão VPN:
 - Adicione uma rota à tabela de rotas de sua sub-rede privada com o gateway privado virtual como destino e a rede (intervalo CIDR) do Windows Server como destino. Para obter mais informações, consulte [Adicionar e remover rotas de uma tabelas](#) no Amazon Virtual Private Cloud - Guia do usuário.
 - Ative a propagação de rotas para o gateway privado virtual. Para ter mais informações, consulte [\(Gateway privado virtual\) Habilitar a propagação de rotas na tabela de rotas](#).
- Crie um grupo de segurança para suas instâncias que permita a comunicação entre a rede e sua VPC:
 - Adicione regras que permitam acesso de entrada RDP ou SSH de sua rede. Isso possibilita que você se conecte de sua rede a instâncias em sua VPC. Por exemplo, para permitir que computadores em sua rede acessem instâncias do Linux em sua VPC, crie uma regra de entrada com um tipo de SSH e o conjunto de fontes para o intervalo CIDR de sua rede (por exemplo, 172.31.0.0/16). Para mais informações, consulte [Grupos de segurança para a VPC](#) no Guia do usuário da Amazon VPC.
 - Adicione uma regra que permita acesso ICMP de entrada de sua rede. Isso possibilita que você teste sua conexão VPN executando ping em uma instância em sua VPC em seu Windows Server.

Etapa 2: Fazer download do arquivo de configuração para a conexão VPN

Você pode usar o console da Amazon VPC para fazer download de um arquivo de configuração do Windows Server para sua conexão VPN.

Para fazer download do arquivo de configuração

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Site-to-Site VPN Connections (Conexões de VPN de local a local).
3. Selecione sua conexão VPN e escolha Download Configuration (Baixar configuração).

4. Selecione Microsoft como fornecedor, Windows Server como plataforma e 2012 R2 como software. Escolha Baixar. Você pode abrir ou salvar o arquivo.

O arquivo de configuração contém uma seção de informações semelhante ao exemplo a seguir. Você vê essas informações apresentadas duas vezes, uma vez para cada túnel.

```
vgw-1a2b3c4d Tunnel1
-----
Local Tunnel Endpoint:      203.0.113.1
Remote Tunnel Endpoint:    203.83.222.237
Endpoint 1:                [Your_Static_Route_IP_Prefix]
Endpoint 2:                [Your_VPC_CIDR_Block]
Preshared key:             xCjNLsLoCmKsakwcdor9yX6GsEXAMPLE
```

Local Tunnel Endpoint

O endereço IP especificado para o gateway do cliente quando criou a conexão VPN.

Remote Tunnel Endpoint

Um dos dois endereços IP do gateway privado virtual que encerra a conexão VPN no AWS lado da conexão.

Endpoint 1

O prefixo de IP especificado como rota estática ao criar a conexão VPN. Esses são os endereços IP em sua rede que têm permissão para usar a conexão VPN para acessar sua VPC.

Endpoint 2

O intervalo de endereços IP (bloco CIDR) da VPC anexado ao gateway privado virtual (por exemplo, 10.0.0.0/16).

Preshared key

A chave pré-compartilhada que é usada para estabelecer a conexão VPN de IPsec entre Local Tunnel Endpoint e Remote Tunnel Endpoint.

Sugerimos que você configure os dois túneis como parte da conexão VPN. Cada túnel se conecta a um concentrador de VPN separado no lado Amazon da conexão VPN. Embora apenas um túnel por vez esteja ativo, o segundo túnel se estabelece automaticamente se o primeiro túnel cair. Ter túneis redundantes garante disponibilidade contínua no caso de uma falha no dispositivo. Pelo fato

de somente um túnel por vez estar disponível, o console da Amazon VPC indica que um túnel está desativado. Como esse comportamento é esperado, nenhuma ação é necessária de sua parte.

Com dois túneis configurados, se ocorrer uma falha no dispositivo AWS, sua conexão VPN automaticamente passará para o segundo túnel do gateway privado virtual em questão de minutos. Ao configurar o dispositivo de gateway do cliente, é importante configurar ambos os túneis.

Note

De tempos em tempos, AWS realiza manutenção de rotina no gateway privado virtual. Essa manutenção pode desabilitar um dos dois túneis da conexão VPN durante um breve espaço de tempo. Sua conexão VPN executa failover automaticamente no segundo túnel enquanto realizamos essa manutenção.

Outras informações sobre o IKE (Internet Key Exchange) e associações de segurança (SA) IPsec são apresentadas no arquivo de configuração baixado.

```
MainModeSecMethods:      DHGroup2-AES128-SHA1
MainModeKeyLifetime:     480min,0sess
QuickModeSecMethods:     ESP:SHA1-AES128+60min+100000kb
QuickModePFS:            DHGroup2
```

MainModeSecMethods

Os algoritmos de criptografia e autenticação da SA IKE. Estas são as configurações sugeridas para conexão VPN e são as configurações padrão para conexões VPN IPsec do Windows Server.

MainModeKeyLifetime

Vida útil da chave SA IKE. Esta é a configuração sugerida para a conexão VPN e é a configuração padrão para conexões VPN IPsec do Windows Server.

QuickModeSecMethods

Os algoritmos de criptografia e autenticação da SA IPsec. Estas são as configurações sugeridas para conexão VPN e são as configurações padrão para conexões VPN IPsec do Windows Server.

QuickModePFS

É aconselhável usar o Perfect Forward Secrecy (PFS - Sigilo de encaminhamento perfeito) da chave mestra para as sessões IPsec.

Etapa 3: configurar o Windows Server

Antes de configurar o túnel VPN, você precisa instalar e configurar os Serviços de Roteamento e Acesso Remoto no Windows Server. Isso permite que os usuários remotos acessem os recursos na rede.

Para instalar os Serviços de Roteamento e Acesso Remoto

1. Faça logon no seu Windows Server.
2. Vá para o menu Start e escolha Server Manager.
3. Instale Serviços de Roteamento e Acesso Remoto:
 - a. No menu Manage, escolha Add Roles and Features.
 - b. Na página Before You Begin, verifique se seu servidor atende aos pré-requisitos e escolha Next.
 - c. Escolha Role-based or feature-based installation e Next.
 - d. Escolha Select a server from the server pool (Selecionar um servidor no pool de servidor), selecione o Windows Server e escolha Next (Avançar).
 - e. Selecione Network Policy and Access Services na lista. Na caixa de diálogo exibida, escolha Add Features para confirmar os recursos necessários para esta função.
 - f. Na mesma lista, escolha Acesso Remoto, Próximo.
 - g. Na página Select features, escolha Next.
 - h. Na página Network Policy and Access Services, escolha Next.
 - i. Na página Remote Access, escolha Next. Na próxima página, selecione DirectAccess VPN (RAS). Na caixa de diálogo exibida, escolha Add Features para confirmar os recursos necessários para este serviço de função. Na mesma lista, selecione Routing e escolha Next.
 - j. Na página Web Server Role (IIS), escolha Next. Deixe a seleção padrão e escolha Next.
 - k. Escolha Instalar. Quando a instalação terminar, escolha Close.

Para configurar e ativar o Servidor de Roteamento e Acesso Remoto

1. No painel, selecione Notifications (Notificações). Deve haver uma tarefa a ser concluída na configuração depois da implantação. Escolha o link Open the Getting Started Wizard.
2. Escolha Deploy VPN only.

3. Na caixa de diálogo Routing and Remote Access (Roteamento e acesso remoto), escolha o nome do servidor, escolha Action (Ação) e Configure and Enable Routing and Remote Access (Configurar e habilitar o roteamento e o acesso remoto).
4. Em Routing and Remote Access Server Setup Wizard, na primeira página, escolha Next.
5. Na página Configuração, escolha Configuração Personalizada, Próximo.
6. Escolha Roteamento de LAN, Próximo, Concluir.
7. Quando solicitado pela caixa de diálogo Routing and Remote Access, escolha Start service.

Etapa 4: Configurar o túnel VPN

Você pode configurar o túnel de VPN executando os scripts netsh incluídos no arquivo de configuração baixado ou usando a interface do usuário do Windows Server.

Important

Sugerimos que você use a chave mestra perfect forward secrecy (PFS) para suas sessões de IPsec. Se você optar por executar o script netsh, ele incluirá um parâmetro para ativar o PFS (`)qmpfs=dhgroup2`. Você não pode habilitar o PFS usando a interface do usuário do Windows — é preciso habilitá-lo usando a linha de comando.

Opções

- [Opção 1: Executar o script netsh](#)
- [Opção 2: Usar a interface de usuário do Windows Server](#)

Opção 1: Executar o script netsh

Copie o script netsh do arquivo de configuração baixado e substitua as variáveis. A seguir encontra-se um exemplo de script.

```
netsh advfirewall consec add rule Name="vgw-1a2b3c4d Tunnel 1" ^
Enable=Yes Profile=any Type=Static Mode=Tunnel ^
LocalTunnelEndpoint=Windows_Server_Private_IP_address ^
RemoteTunnelEndpoint=203.83.222.236 Endpoint1=Your_Static_Route_IP_Prefix ^
Endpoint2=Your_VPC_CIDR_Block Protocol=Any Action=RequireInClearOut ^
Auth1=ComputerPSK Auth1PSK=xCjNLSLoCmKsakwcdor9yX6GsEXAMPLE ^
QMSecMethods=ESP:SHA1-AES128+60min+100000kb ^
```

```
ExemptIPsecProtectedConnections=No ApplyAuthz=No QMPFS=dhgroup2
```

Name: Você pode substituir o nome sugerido (vgw-1a2b3c4d Tunnel 1) por um nome de sua escolha.

LocalTunnelEndpoint: insira o endereço IP privado do Windows Server na sua rede.

Endpoint1: o bloco CIDR da sua rede em que o Windows Server reside, por exemplo, 172.31.0.0/16. Cerque esse valor com aspas duplas ("").

Endpoint2: o bloco CIDR da sua VPC ou uma sub-rede na sua VPC, por exemplo, 10.0.0.0/16. Cerque esse valor com aspas duplas ("").

Execute o script atualizado em uma janela do prompt de comando no Windows Server. (O sinal ^ permite que você corte e cole o texto contornado na linha de comando.) Para configurar o segundo túnel VPN para essa conexão VPN, repita o processo usando o segundo script netsh no arquivo de configuração.

Quando terminar, vá para [Configurar o firewall do Windows](#).

Para obter mais informações sobre os parâmetros netsh, consulte [Comandos Netsh AdvFirewall Consec](#) na Microsoft Library. TechNet

Opção 2: Usar a interface de usuário do Windows Server

Você pode também usar a interface do usuário do Windows Server para configurar o túnel de VPN.

Important

Você não pode habilitar o Perfect Forward Secrecy (PFS - "sigilo encaminhado") da chave mestra usando a interface do usuário do Windows Server. Você precisa habilitar o PFS usando a linha de comando, conforme descrito em [Habilitar sigredo de encaminhamento perfeito da chave mestra](#).

Tarefas

- [Configurar uma regra de segurança para um túnel de VPN](#)
- [Confirmar a configuração do túnel](#)
- [Habilitar sigredo de encaminhamento perfeito da chave mestra](#)
- [Configurar o firewall do Windows](#)

Configurar uma regra de segurança para um túnel de VPN

Nesta seção, você configurará uma regra de segurança no Windows Server para criar um túnel de VPN.

Para configurar uma regra de segurança para um túnel VPN

1. Abra o Gerenciador do Servidor, escolha Tools (Ferramentas) e selecione Windows Firewall with Advanced Security (Firewall do Windows com Segurança Avançada).
2. Selecione Connection Security Rules, escolha Action e New Rule.
3. No assistente New Connection Security Rule (Nova Regra de Segurança de Conexão) da página Rule Type (Tipo de regra), selecione Tunnel (Túnel) e Next (Próximo).
4. Na página Tunnel Type (Tipo de túnel), em What type of tunnel would you like to create (Qual tipo de túnel gostaria de criar), selecione Custom configuration (Configuração personalizada). Em Gostaria de isentar as conexões protegidas por IPsec deste túnel, deixe o valor padrão marcado selecionado (Não. Envie todo o tráfego de rede correspondente a essa regra de segurança de conexão pelo túnel) e escolha Próximo.
5. Na página Requisitos, escolha Exigir autenticação para conexões de entrada. Não estabeleça túneis para conexões de saída e escolha Avançar.
6. Na página Tunnel Endpoints (Endpoints de túnel), em Which computers are in Endpoint 1 (Quais computadores estão no endpoint 1), escolha Add (Adicionar). Insira o intervalo CIDR da sua rede (atrás do dispositivo de gateway do cliente do Windows Server; por exemplo, 172.31.0.0/16) e escolha OK. O intervalo pode incluir o endereço IP do dispositivo de gateway do cliente.
7. Em What is the local tunnel endpoint (closest to computer in Endpoint 1), escolha Edit. No campo IPv4 address (endereço IPv4), digite o endereço IP privado do Windows Server e escolha OK.
8. Em What is the remote tunnel endpoint (closest to computers in Endpoint 2), escolha Edit. No campo IPv4 address, digite o endereço IP do gateway privado virtual para o túnel 1 do arquivo de configuração (consulte Remote Tunnel Endpoint) e escolha OK.

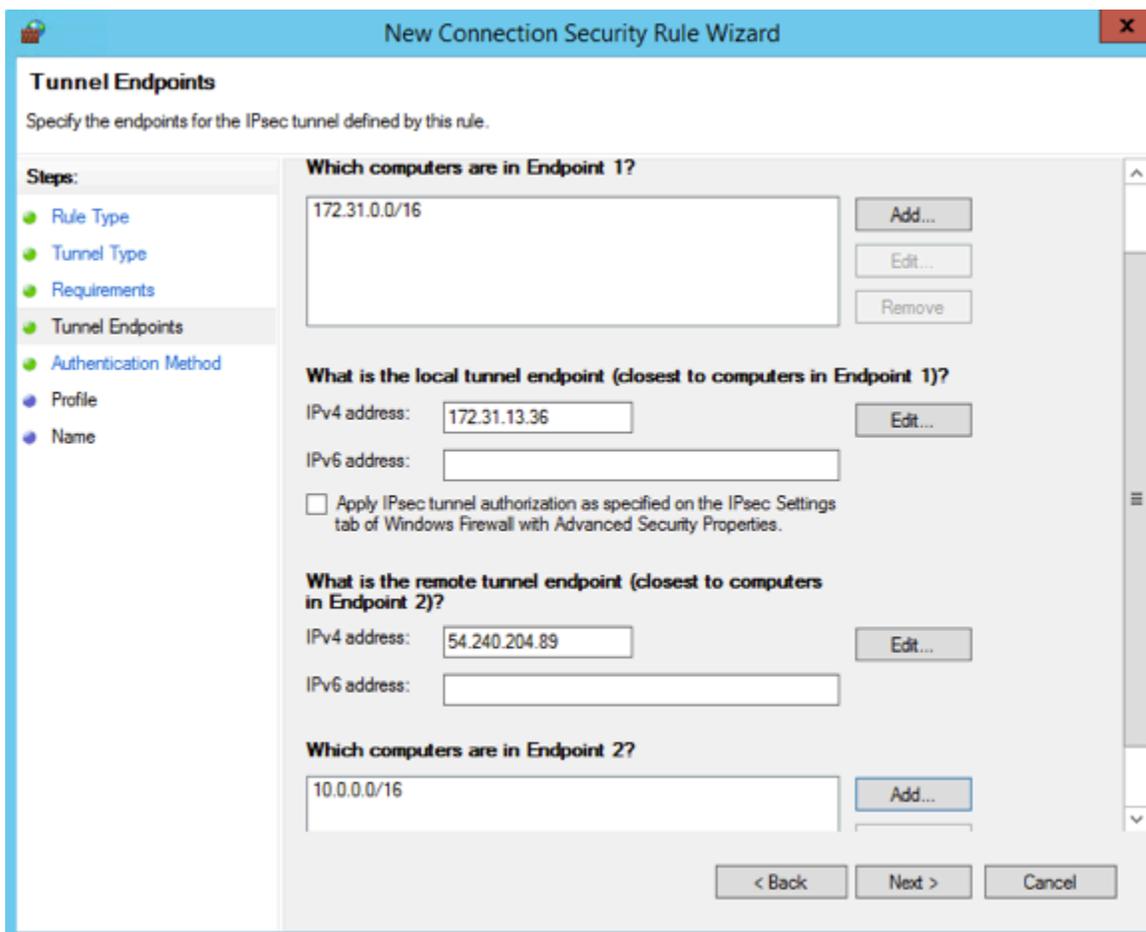
Important

Se você estiver repetindo este procedimento para o túnel 2, certifique-se de selecionar o endpoint para o túnel 2.

- Em Which computers are in Endpoint 2, escolha Add. Em This IP address or subnet field, digite o bloco CIDR da VPC e escolha OK.

⚠ Important

Você precisa rolar para baixo na caixa de diálogo até localizar Which computers are in Endpoint 2. Não escolha Next até ter concluído esta etapa, caso contrário, não poderá se conectar ao servidor.



- Confirme se todas as configurações especificadas estão corretas e escolha Next (Próximo).
- Na página Método de Autenticação, selecione Avançado e escolha Personalizar.
- Em First authentication methods, escolha Add.
- Selecione Preshared key (Chave pré-compartilhada), insira o valor da chave pré-compartilhada do arquivo de configuração e escolha OK.

⚠ Important

Se você estiver repetindo este procedimento para o túnel 2, certifique-se de selecionar a chave pré-compartilhada para o túnel 2.

14. Certifique-se de que First authentication is optional não esteja selecionada e escolha OK.
15. Escolha Próximo.
16. Na página Perfil, marque todas as três caixas de seleção: Domínio, Privado e Público. Escolha Próximo.
17. Na página Name (Nome), digite um nome para a regra de conexão, por exemplo, VPN to Tunnel 1 e escolha Finish (Concluir).

Repita o procedimento anterior especificando os dados para o túnel 2 de seu arquivo de configuração.

Assim que concluir, terá dois túneis configurados para sua conexão VPN.

Confirmar a configuração do túnel

Para confirmar a configuração do túnel

1. Abra o Server Manager, escolha Tools, selecione Windows Firewall with Advanced Security e Connection Security Rules.
2. Verifique o seguinte para os dois túneis:
 - Enabled (Habilitado) está como Yes
 - Endpoint 1 é o bloco CIDR para a rede
 - Endpoint 2 é o bloco CIDR da VPC
 - Authentication mode (Modo de autenticação) é Require inbound and clear outbound.
 - Authentication method (Método de autenticação) é Custom
 - Endpoint 1 port (Porta do endpoint 1) é Any
 - Endpoint 2 port (Porta do endpoint 2) é Any
 - Protocol (Protocolo) é Any
3. Selecione a primeira regra e escolha Properties.

4. Na guia Authentication (Autenticação) em Method (Método), escolha Customize (Personalizar). Verifique se a opção First authentication methods (Primeiros métodos de autenticação) contém a chave pré-compartilhada correta do arquivo de configuração para o túnel e escolha OK.
5. Na guia Advanced (Avançado), verifique se Domain (Domínio), Private (Privado) e Public (Público) estão todos selecionados.
6. Em IPsec tunneling, escolha Customize. Verifique as seguintes configurações de túnel IPsec, escolha OK e OK novamente para fechar a caixa de diálogo.
 - Use IPsec tunneling (Usar encapsulamento IPsec) está selecionada.
 - Local tunnel endpoint (closest to Endpoint 1) (Ponto de extremidade de túnel local (mais próximo ao Ponto de Extremidade 1)) contém o endereço IP do Windows Server. Se o dispositivo de gateway do cliente for uma instância do EC2, esse será o endereço IP privado da instância.
 - Remote tunnel endpoint (closest to Endpoint 2) (Ponto de extremidade de túnel remoto [mais próximo ao Ponto de Extremidade 2]) contém o endereço IP do gateway privado virtual para esse túnel.
7. Abra as propriedades para o segundo túnel. Repita as etapas 4 a 7 para esse túnel.

Habilitar sigredo de encaminhamento perfeito da chave mestra

Você pode habilitar o Perfect Forward Secrecy (PFS - Sigilo de encaminhamento perfeito) da chave mestra usando a linha de comando. Você não pode habilitar esse recurso usando a interface do usuário.

Para habilitar o Perfect Forward Secrecy (PFS - Sigilo de encaminhamento perfeito) da chave mestra

1. No Windows Server, abra uma nova janela do prompt de comando.
2. Insira o comando a seguir, substituindo `rule_name` pelo nome que você deu à primeira regra de conexão.

```
netsh advfirewall consec set rule name="rule_name" new QMPFS=dhgroup2
QMPSecMethods=ESP:SHA1-AES128+60min+100000kb
```

3. Repita a etapa 2 para o segundo túnel, desta vez substituindo `rule_name` pelo nome que você deu à segunda regra de conexão.

Configurar o firewall do Windows

Assim que configurar suas regras de segurança em seu servidor, defina algumas configurações básicas de IPsec para trabalhar com o gateway privado virtual.

Para configurar o Firewall do Windows

1. Abra o Gerenciador do Servidor, escolha Tools (Ferramentas), selecione Windows Defender Firewall with Advanced Security (Firewall do Windows Defender com Segurança Avançada) e escolha Properties (Propriedades).
2. Na guia IPsec Settings, em IPsec exemptions, verifique se Exempt ICMP from IPsec está como No (default). Verifique se IPsec tunnel authorization está como None.
3. Em IPsec defaults, escolha Customize.
4. Em Key exchange (Main Mode), selecione Advanced e Customize.
5. Em Customize Advanced Key Exchange Settings (Personalizar configurações de troca de chaves avançada), sob Security methods (Métodos de segurança), verifique se os seguintes valores padrão são usados para a primeira entrada:
 - Integridade: SHA-1
 - Criptografia: AES-CBC 128
 - Algoritmo de troca de chaves: Grupo Diffie-Hellman 2
 - Em Key lifetimes, verifique se Minutes está 480 e se Sessions está 0.

Essas configurações correspondem às seguintes entradas no arquivo de configuração:

```
MainModeSecMethods: DHGroup2-AES128-SHA1,DHGroup2-3DES-SHA1
MainModeKeyLifetime: 480min,0sec
```

6. Em Key exchange options, selecione Use Diffie-Hellman for enhanced security e escolha OK.
7. Em Data protection (Quick Mode), selecione Advanced e Customize.
8. Selecione Require encryption for all connection security rules that use these settings.
9. Em Data integrity and encryption, deixe os valores padrão:
 - Protocolo: ESP
 - Integridade: SHA-1
 - Criptografia: AES-CBC 128

- Tempo de vida: 60 minutos

Esses valores correspondem à seguinte entrada no arquivo de configuração.

```
QuickModeSecMethods:  
ESP:SHA1-AES128+60min+100000kb
```

10. Escolha OK para retornar à caixa de diálogo Personalizar Configurações de IPsec, e escolha OK novamente para salvar a configuração.

Etapa 5: Habilitar a detecção de gateway inativo

Em seguida, configure o TCP para detectar quando um gateway fica indisponível. Você pode fazer isso, modificando esta chave de registro: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters. Não execute esta etapa enquanto não concluir as seções precedentes. Assim que alterar a chave de registro, deverá reinicializar o servidor.

Para habilitar a detecção de gateway inativo

1. No Windows Server, inicie o prompt de comando ou uma PowerShell sessão e digite regedit para iniciar o Editor do Registro.
2. Expanda HKEY_LOCAL_MACHINE, expanda SYSTEM, expanda, expanda Serviços, expanda Tcpip e CurrentControlSet, em seguida, expanda Parâmetros.
3. No menu Edit, selecione New e DWORD (32-bit) Value.
4. Insira o nome EnableDeadGWDetect.
5. Selecione EnableDeadGWDetect e escolha Editar, Modificar.
6. Em Value data, digite 1 e escolha OK.
7. Feche o Registry Editor e reinicie o servidor.

Para obter mais informações, consulte [EnableDeadGWDetect](#) na Microsoft TechNet Library.

Etapa 6: Testar a conexão VPN

Para testar se a conexão VPN está funcionando corretamente, execute uma instância em sua VPC e garanta que ela não tenha uma conexão com a Internet. Assim que executar a instância, execute ping no respectivo endereço IP privado no Windows Server. O túnel VPN é ativado quando tráfego

é gerado no dispositivo de gateway do cliente. Portanto, o comando ping também inicia a conexão VPN.

Para obter as etapas para testar a conexão VPN, consulte [Testar uma conexão do Site-to-Site VPN](#).

Se o comando ping falhar, verifique as seguintes informações:

- Confira se você configurou as regras de security group para permitir ICMP na instância de sua VPC. Se o Windows Server for uma instância do EC2, confirme se as regras de saída do respectivo grupo de segurança permitem tráfego IPsec. Para ter mais informações, consulte [Configurar a instância do Windows](#).
- Confirme se o sistema operacional da instância em que você está executando ping está configurada para responder a ICMP. Recomendamos que você use uma das Amazon Linux AMIs.
- Se a instância em que estiver executando ping for uma instância do Windows, conecte-se a ela e habilite ICMPv4 de entrada no firewall do Windows.
- Verifique se configurou as tabelas de rota corretamente para a sua VPC ou sub-rede. Para ter mais informações, consulte [Etapa 1: Criar uma conexão VPN e configurar a VPC](#).
- Se o dispositivo de gateway do cliente for uma instância do EC2, verifique se você desativou a verificação de origem/destino da instância. Para ter mais informações, consulte [Configurar a instância do Windows](#).

No console da Amazon VPC, na página VPN Connections, selecione sua conexão VPN. O primeiro túnel encontra-se no estado ATIVO. O segundo túnel deve ser configurado, mas ele só será usado se o primeiro ficar inativo. Pode demorar alguns instantes para estabelecer os túneis criptografados.

Solução de problemas do dispositivo de gateway do cliente

Ao solucionar problemas com seu dispositivo de gateway do cliente, é importante ter uma abordagem estruturada. Os dois primeiros tópicos desta seção fornecem fluxogramas generalizados para solucionar problemas ao usar um dispositivo configurado para roteamento dinâmico (BGP ativado) e um dispositivo configurado para roteamento estático (sem BGP habilitado), respectivamente. A seguir esses tópicos, estão os guias de solução de problemas específicos do dispositivo para dispositivos de gateway de clientes Cisco, Juniper e Yamaha.

Além dos tópicos desta seção, habilitar [AWS Site-to-Site VPN troncos](#) pode ser muito útil para solucionar problemas de VPN conectividade. Para obter instruções gerais de teste, consulte também [Testar uma conexão do Site-to-Site VPN](#).

Tópicos

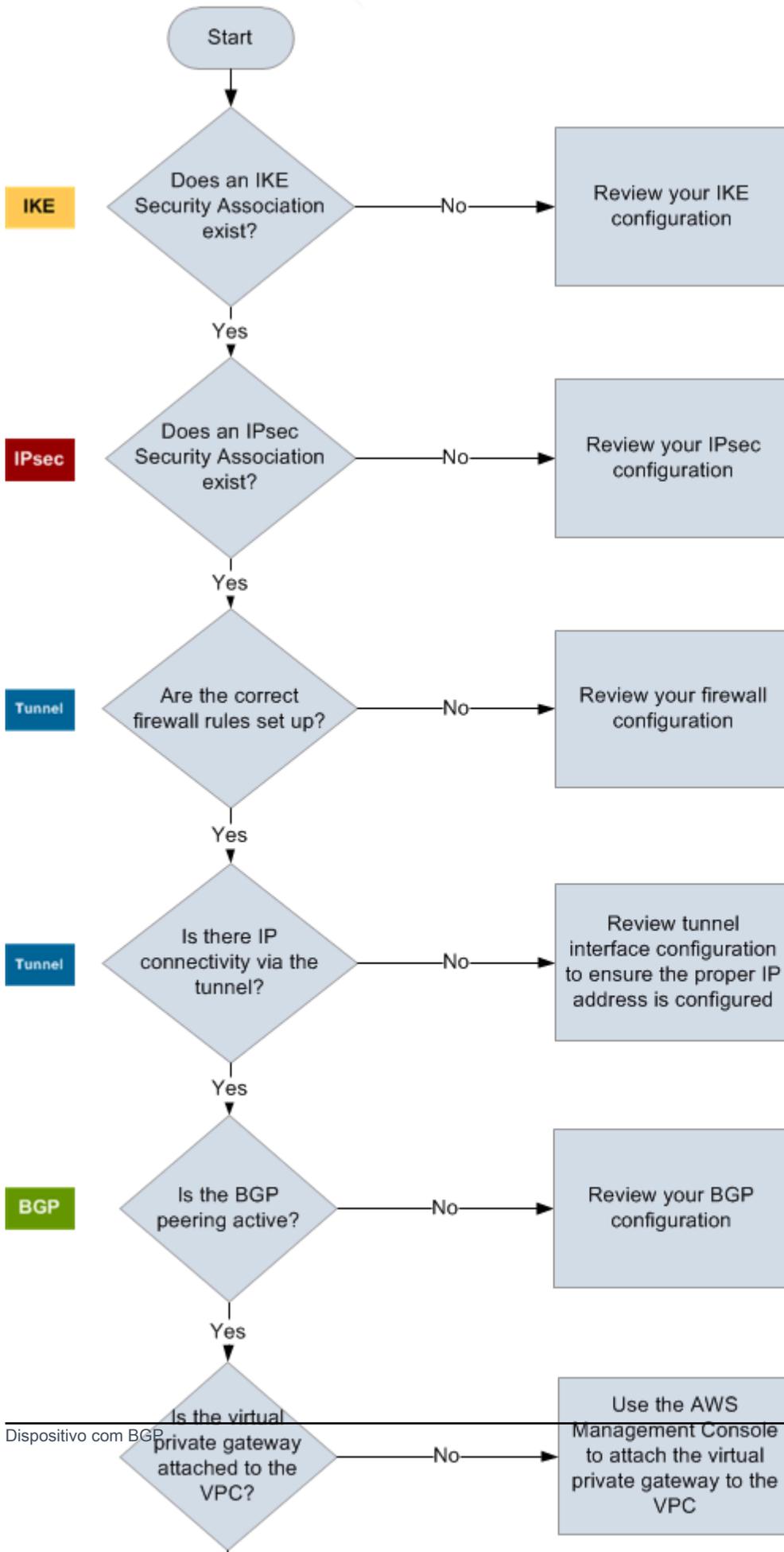
- [Solução de problemas de conectividade ao usar o Border Gateway Protocol](#)
- [Solução de problemas de conectividade sem Border Gateway Protocol](#)
- [Solução de problemas de conectividade do dispositivo Cisco ASA Customer Gate](#)
- [Solução de problemas de conectividade do dispositivo Cisco IOS Customer Gate](#)
- [Solução de problemas do dispositivo Cisco IOS Customer Gateway sem conectividade com o Border Gateway](#)
- [Solução de problemas de conectividade do dispositivo de gateway do cliente do Juniper JunOS](#)
- [Solução de problemas de conectividade de gateway do cliente do Juniper ScreenOS](#)
- [Solução de problemas de conectividade do dispositivo de gateway do cliente da Yamaha](#)

Recursos adicionais

- [VPC Fórum da Amazon](#)
- [Como soluciono problemas de conectividade de VPN túneis com minha AmazonVPC?](#)

Solução de problemas de conectividade ao usar o Border Gateway Protocol

O diagrama e a tabela a seguir fornecem instruções gerais para solucionar problemas em um dispositivo de gateway do cliente que usa o Border Gateway Protocol (BGP). Também recomendamos que você habilite os recursos de depuração do dispositivo. Consulte o fornecedor do dispositivo do gateway para obter informações detalhadas.



IKE	<p>Determine se existe uma associação de IKE segurança.</p> <p>É necessária uma associação de IKE segurança para trocar as chaves usadas para estabelecer a associação IPsec de segurança.</p> <p>Se não existir nenhuma associação de IKE segurança, revise suas IKE configurações. É necessário configurar os parâmetros de criptografia, autenticação, sigilo de encaminhamento perfeito e modo, conforme listado no arquivo de configuração.</p> <p>Se existir uma associação de IKE segurança, vá para 'IPsec'.</p>
IPsec	<p>Determine se existe uma associação de IPsec segurança (SA).</p> <p>Um IPsec SA é o túnel em si. Consulte seu dispositivo de gateway do cliente para determinar se um IPsec SA está ativo. Configure os parâmetros de criptografia, autenticação, sigilo de encaminhamento perfeito e modo, conforme listado no arquivo de configuração.</p> <p>Se não existir nenhum IPsec SA, revise sua IPsec configuração.</p> <p>Se existir um IPsec SA, vá para “Túnel”.</p>
Túnel	<p>Confirme se as regras necessárias de firewall estão configuradas (para obter uma lista de regras, consulte Regras de firewall para seu dispositivo de gateway do cliente). Se não, prossiga.</p> <p>Determine se existe conectividade IP por meio do túnel.</p> <p>Cada lado do túnel tem um endereço IP conforme especificado no arquivo de configuração. O endereço do gateway privado virtual é o endereço usado como endereço do BGP vizinho. No dispositivo de gateway do cliente, execute ping nesse endereço para determinar se o tráfego de IP está sendo criptografado e descriptografado adequadamente.</p> <p>Se o ping não tiver êxito, revise a configuração da interface do túnel para verificar se o endereço IP apropriado está configurado.</p> <p>Se o ping for bem-sucedido, vá para 'BGP'.</p>
BGP	<p>Determine se a sessão de BGP emparelhamento está ativa.</p>

Para cada túnel, faça o seguinte:

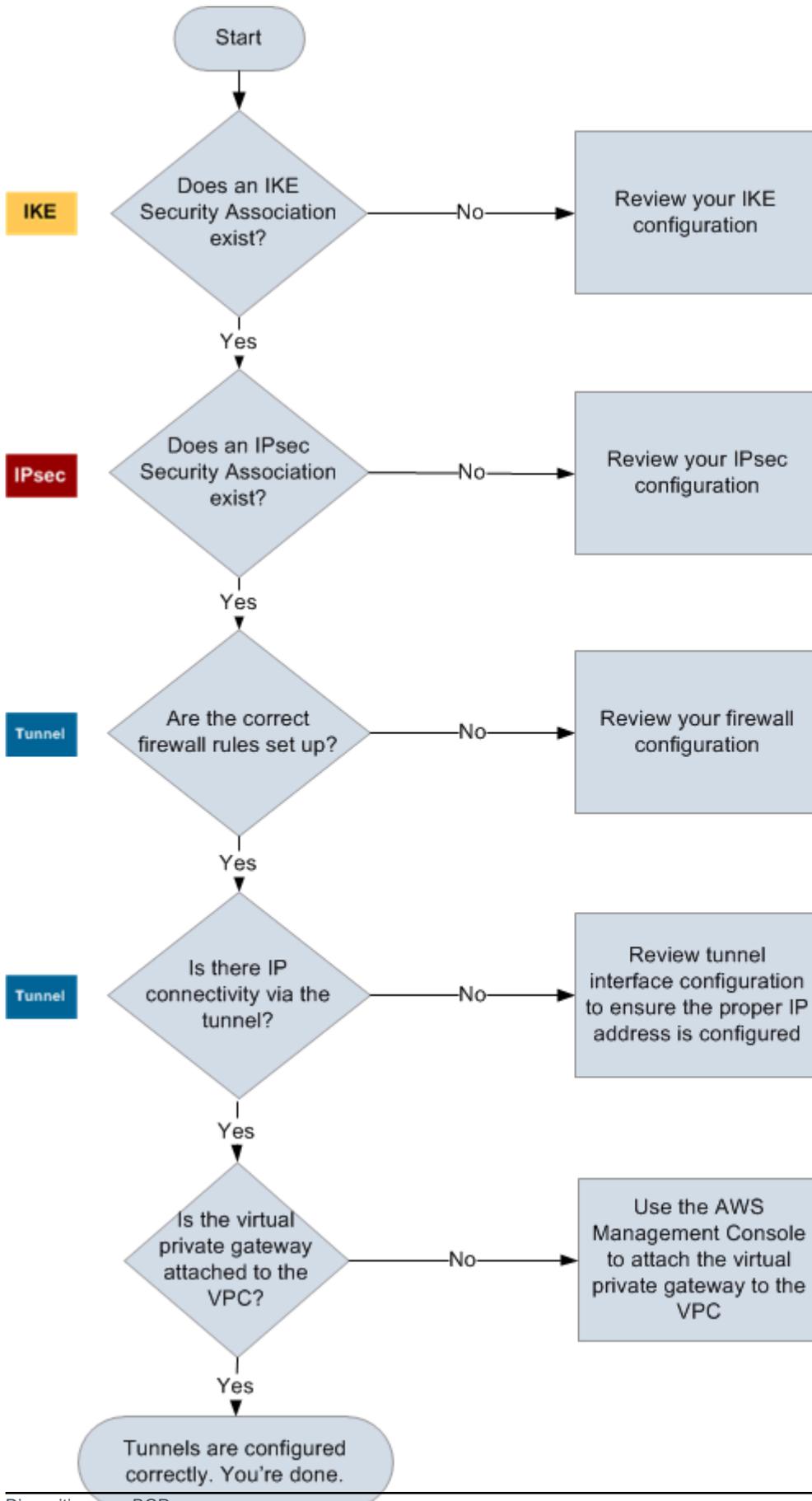
- Em seu dispositivo de gateway do cliente, determine se o BGP status é `Active` ou `Established` . Pode levar aproximadamente 30 segundos para que um BGP peering se torne ativo.
- Confirme se o dispositivo de gateway do cliente está anunciando a rota padrão (0.0.0.0/0) para o gateway privado virtual.

Se os túneis não estiverem nesse estado, revise sua BGP configuração.

Se o BGP peering for estabelecido, você estiver recebendo um prefixo e anunciando um prefixo, seu túnel será configurado corretamente. Certifique-se de que os dois túneis estão nesse estado.

Solução de problemas de conectividade sem Border Gateway Protocol

O diagrama e a tabela a seguir fornecem instruções gerais para solucionar problemas em um dispositivo de gateway do cliente que não usa o Border Gateway Protocol (BGP). Também recomendamos que você habilite os recursos de depuração do dispositivo. Consulte o fornecedor do dispositivo do gateway para obter informações detalhadas.



IKE	<p>Determine se existe uma associação de IKE segurança.</p> <p>É necessária uma associação de IKE segurança para trocar as chaves usadas para estabelecer a associação IPsec de segurança.</p> <p>Se não existir nenhuma associação de IKE segurança, revise suas IKE configurações. É necessário configurar os parâmetros de criptografia, autenticação, sigilo de encaminhamento perfeito e modo, conforme listado no arquivo de configuração.</p> <p>Se existir uma associação de IKE segurança, vá para 'IPsec'.</p>
IPsec	<p>Determine se existe uma associação de IPsec segurança (SA).</p> <p>Um IPsec SA é o túnel em si. Consulte seu dispositivo de gateway do cliente para determinar se um IPsec SA está ativo. Configure os parâmetros de criptografia, autenticação, sigilo de encaminhamento perfeito e modo, conforme listado no arquivo de configuração.</p> <p>Se não existir nenhum IPsec SA, revise sua IPsec configuração.</p> <p>Se existir um IPsec SA, vá para "Túnel".</p>
Túnel	<p>Confirme se as regras necessárias de firewall estão configuradas (para obter uma lista de regras, consulte Regras de firewall para seu dispositivo de gateway do cliente). Se não, prossiga.</p> <p>Determine se existe conectividade IP por meio do túnel.</p> <p>Cada lado do túnel tem um endereço IP conforme especificado no arquivo de configuração. O endereço do gateway privado virtual é o endereço usado como endereço do BGP vizinho. No dispositivo de gateway do cliente, execute ping nesse endereço para determinar se o tráfego de IP está sendo criptografado e descriptografado adequadamente.</p> <p>Se o ping não tiver êxito, revise a configuração da interface do túnel para verificar se o endereço IP apropriado está configurado.</p> <p>Se o ping for bem-sucedido, avance para "Rotas estáticas".</p>

Rotas estáticas

Para cada túnel, faça o seguinte:

- Verifique se você adicionou uma rota estática à sua VPC CIDR com os túneis como o próximo salto.
- Verifique se você adicionou uma rota estática no VPC console da Amazon, para que o gateway privado virtual direcione o tráfego de volta para suas redes internas.

Se os túneis não estiverem nesse estado, revise a configuração de seu dispositivo.

Verifique se ambos os túneis estão nesse estado. Se sim, você terá terminado.

Solução de problemas de conectividade do dispositivo Cisco ASA Customer Gate

Ao solucionar problemas de conectividade de um dispositivo Cisco Customer Gateway IKEIPsec, considere o roteamento. Você pode solucionar essas áreas em qualquer ordem, mas recomendamos que comece com IKE (na parte inferior da pilha de rede) e suba.

Important

Alguns Cisco suportam ASAs apenas o modo ativo/em espera. Quando você usa esses CiscoASAs, você pode ter somente um túnel ativo por vez. O outro túnel em espera ficará ativo somente se o primeiro túnel ficar indisponível. O túnel em espera pode gerar o seguinte erro nos arquivos de log, o qual pode ser ignorado: `Rejecting IPSec tunnel: no matching crypto map entry for remote proxy 0.0.0.0/0.0.0.0/0/0 local proxy 0.0.0.0/0.0.0.0/0/0 on interface outside.`

IKE

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IKE configurado corretamente.

```
ciscoasa# show crypto isakmp sa
```

```

Active SA: 2
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1  IKE Peer: AWS_ENDPOINT_1
   Type    : L2L                Role    : initiator
   Rekey   : no                 State   : MM_ACTIVE

```

Você deve ver uma ou mais linhas contendo um valor de `src` do gateway remoto especificado nos túneis. O valor de `state` deve ser `MM_ACTIVE` e o `status` deve ser `ACTIVE`. A ausência de uma entrada, ou de qualquer entrada em outro estado, indica que ela não IKE está configurada corretamente.

Para solucionar outros problemas, execute os comandos a seguir para ativar mensagens de log que fornecem informações de diagnóstico.

```

router# term mon
router# debug crypto isakmp

```

Para desativar a depuração, use o comando a seguir.

```

router# no debug crypto isakmp

```

IPsec

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IPsec configurado corretamente.

```

ciscoasa# show crypto ipsec sa

```

```

interface: outside
  Crypto map tag: VPN_crypto_map_name, seq num: 2, local addr: 172.25.50.101

  access-list integ-ppe-loopback extended permit ip any vpc_subnet subnet_mask
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (vpc_subnet/subnet_mask/0/0)
  current_peer: integ-ppel

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

```

```
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.25.50.101, remote crypto endpt.: AWS_ENDPOINT_1

path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: 6D9F8D3B
current inbound spi : 48B456A6

inbound esp sas:
spi: 0x48B456A6 (1219778214)
  transform: esp-aes esp-sha-hmac no compression
  in use settings = {L2L, Tunnel, PFS Group 2, }
  slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
  sa timing: remaining key lifetime (kB/sec): (4374000/3593)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
outbound esp sas:
spi: 0x6D9F8D3B (1839172923)
  transform: esp-aes esp-sha-hmac no compression
  in use settings = {L2L, Tunnel, PFS Group 2, }
  slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
  sa timing: remaining key lifetime (kB/sec): (4374000/3593)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
```

Para a interface de cada túnel, você deve ver inbound esp sas e outbound esp sas. Isso pressupõe que uma SA esteja listada (por exemplo, spi : 0x48B456A6) e que IPsec esteja configurada corretamente.

Na CiscoASA, isso IPsec só aparece após o envio de tráfego interessante (tráfego que deveria ser criptografado). Para manter sempre o IPsec ativo, recomendamos configurar um SLA monitor. O SLA monitor continua enviando tráfego interessante, mantendo o IPsec ativo.

Você também pode usar o seguinte comando ping para forçá-lo IPsec a iniciar a negociação e subir.

```
ping ec2_instance_ip_address
```

Pinging *ec2_instance_ip_address* with 32 bytes of data:

```
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
```

```
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
```

```
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
```

Ping statistics for 10.0.0.4:

```
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
```

Approximate round trip times in milliseconds:

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Para solucionar outros problemas, use o comando a seguir para ativar a depuração.

```
router# debug crypto ipsec
```

Para desativar a depuração, use o comando a seguir.

```
router# no debug crypto ipsec
```

Roteamento

Execute ping na outra extremidade do túnel. Se isso estiver funcionando, você IPsec deve estar estabelecido. Se isso não estiver funcionando, verifique suas listas de acesso e consulte a IPsec seção anterior.

Se não conseguir acessar as instâncias, verifique as seguintes informações:

1. Verifique se a lista de acesso está configurada para permitir tráfego associado ao mapa de criptografia.

É possível fazer isso usando o comando a seguir.

```
ciscoasa# show run crypto
```

```
crypto ipsec transform-set transform-amzn esp-aes esp-sha-hmac  
crypto map VPN_crypto_map_name 1 match address access-list-name  
crypto map VPN_crypto_map_name 1 set pfs
```

```
crypto map VPN_crypto_map_name 1 set peer AWS_ENDPOINT_1 AWS_ENDPOINT_2  
crypto map VPN_crypto_map_name 1 set transform-set transform-amzn  
crypto map VPN_crypto_map_name 1 set security-association lifetime seconds 3600
```

2. Verifique a lista de acesso usando o comando a seguir.

```
ciscoasa# show run access-list access-list-name
```

```
access-list access-list-name extended permit ip any vpc_subnet subnet_mask
```

3. Verifique se a lista de acesso está correta. O exemplo de lista de acesso a seguir permite todo o tráfego interno para a VPC sub-rede 10.0.0.0/16.

```
access-list access-list-name extended permit ip any 10.0.0.0 255.255.0.0
```

4. Execute um traceroute a partir do ASA dispositivo Cisco, para ver se ele alcança os roteadores da Amazon (por exemplo, *AWS_ENDPOINT_1/AWS_ENDPOINT_2*).

Se isso chegar ao roteador da Amazon, verifique as rotas estáticas que você adicionou no VPC console da Amazon e também os grupos de segurança das instâncias específicas.

5. Para solucionar outros problemas, revise a configuração.

Solução de problemas de conectividade do dispositivo Cisco IOS Customer Gate

Ao solucionar problemas de conectividade de um dispositivo Cisco Customer Gateway, considere quatro coisas: IKEIPsec,, o túnel e. BGP Você pode solucionar essas áreas em qualquer ordem, mas recomendamos que comece com IKE (na parte inferior da pilha de rede) e suba.

IKE

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IKE configurado corretamente.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA  
dst          src          state          conn-id slot status  
192.168.37.160 72.21.209.193 QM_IDLE          2001    0 ACTIVE
```

```
192.168.37.160 72.21.209.225 QM_IDLE 2002 0 ACTIVE
```

Você deve ver uma ou mais linhas contendo um valor de `src` do gateway remoto especificado nos túneis. O `state` deve ser `QM_IDLE` e o `status` deve ser `ACTIVE`. A ausência de uma entrada, ou de qualquer entrada em outro estado, indica que ela não IKE está configurada corretamente.

Para solucionar outros problemas, execute os comandos a seguir para ativar mensagens de log que fornecem informações de diagnóstico.

```
router# term mon  
router# debug crypto isakmp
```

Para desativar a depuração, use o comando a seguir.

```
router# no debug crypto isakmp
```

IPsec

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IPsec configurado corretamente.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1  
  Crypto map tag: Tunnel1-head-0, local addr 192.168.37.160  
  
  protected vrf: (none)  
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)  
  current_peer 72.21.209.225 port 500  
    PERMIT, flags={origin_is_acl,}  
  #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149  
  #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146  
  #pkts compressed: 0, #pkts decompressed: 0  
  #pkts not compressed: 0, #pkts compr. failed: 0  
  #pkts not decompressed: 0, #pkts decompress failed: 0  
  #send errors 0, #recv errors 0  
  
  local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.225  
  path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0  
  current outbound spi: 0xB8357C22(3090512930)
```

```
inbound esp sas:
spi: 0x6ADB173(112046451)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4467148/3189)
IV size: 16 bytes
replay detection support: Y replay window size: 128
Status: ACTIVE
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
spi: 0xB8357C22(3090512930)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4467148/3189)
IV size: 16 bytes
replay detection support: Y replay window size: 128
Status: ACTIVE
```

```
outbound ah sas:
```

```
outbound pcp sas:
```

```
interface: Tunnel2
```

```
Crypto map tag: Tunnel2-head-0, local addr 174.78.144.73
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
current_peer 72.21.209.193 port 500
```

```
PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
```

```
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.193
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 0xF59A3FF6(4120526838)

inbound esp sas:
spi: 0xB6720137(3060924727)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
sa timing: remaining key lifetime (k/sec): (4387273/3492)
IV size: 16 bytes
replay detection support: Y  replay window size: 128
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF59A3FF6(4120526838)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
sa timing: remaining key lifetime (k/sec): (4387273/3492)
IV size: 16 bytes
replay detection support: Y  replay window size: 128
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

Para a interface de cada túnel, você deve ver `inbound esp sas` e `outbound esp sas`. Supondo que um SA esteja `spi: 0xF95D2F3C` listado (por exemplo) e `Status IPsec` esteja `ACTIVE` configurado corretamente.

Para solucionar outros problemas, use o comando a seguir para ativar a depuração.

```
router# debug crypto ipsec
```

Use o comando a seguir para desativar a depuração.

```
router# no debug crypto ipsec
```

Túnel

Primeiro, verifique se você implementou as regras de firewall necessárias. Para obter mais informações, consulte [Regras de firewall para seu dispositivo de gateway do cliente](#).

Se as regras de firewall estiverem configuradas corretamente, dê prosseguimento à solução de problemas com o comando a seguir.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.255.2/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 72.21.209.225
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Verifique se o `line protocol` está em execução. Verifique se o endereço IP de origem, a interface de origem e o destino correspondem respectivamente à configuração do túnel para o endereço IP externo do dispositivo de gateway do cliente, à interface e ao endereço IP externo do gateway privado virtual. Verifique se o `Tunnel protection via IPSec` está presente. Execute o

comando em ambas as interfaces do túnel. Para resolver qualquer problema, revise a configuração e verifique as conexões físicas com o dispositivo de gateway do cliente.

Além disso, use o comando a seguir e substitua 169.254.255.1 pelo endereço IP interno de seu gateway privado virtual.

```
router# ping 169.254.255.1 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.255.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!!
```

Você deve ver cinco pontos de exclamação.

Para solucionar outros problemas, revise a configuração.

BGP

Use o seguinte comando.

```
router# show ip bgp summary
```

```
BGP router identifier 192.168.37.160, local AS number 65000
BGP table version is 8, main routing table version 8
2 network entries using 312 bytes of memory
2 path entries using 136 bytes of memory
3/1 BGP path/bestpath attribute entries using 444 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 948 total bytes of memory
BGP activity 4/1 prefixes, 4/1 paths, scan interval 15 secs
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
169.254.255.1	4	7224	363	323	8	0	0	00:54:21	1
169.254.255.5	4	7224	364	323	8	0	0	00:00:24	1

Ambos os vizinhos deve ser listados. Para cada um, você deve ver um valor State/PfxRcd de 1.

Se o BGP peering estiver ativo, verifique se o dispositivo de gateway do cliente está anunciando a rota padrão (0.0.0.0/0) para o VPC

```
router# show bgp all neighbors 169.254.255.1 advertised-routes
```

```
For address family: IPv4 Unicast
BGP table version is 3, local router ID is 174.78.144.73
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

Network          Next Hop          Metric   LocPrf Weight Path
*> 10.120.0.0/16 169.254.255.1     100      0   7224   i

Total number of prefixes 1
```

Além disso, verifique se você está recebendo o prefixo correspondente ao seu VPC do gateway privado virtual.

```
router# show ip route bgp
```

```
10.0.0.0/16 is subnetted, 1 subnets
B       10.255.0.0 [20/0] via 169.254.255.1, 00:00:20
```

Para solucionar outros problemas, revise a configuração.

Solução de problemas do dispositivo Cisco IOS Customer Gateway sem conectividade com o Border Gateway

Ao solucionar problemas de conectividade de um dispositivo Cisco Customer Gateway, considere três coisas: IKEIPsec, e túnel. Você pode solucionar essas áreas em qualquer ordem, mas recomendamos que comece com IKE (na parte inferior da pilha de rede) e suba.

IKE

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IKE configurado corretamente.

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
174.78.144.73 205.251.233.121 QM_IDLE        2001    0 ACTIVE
174.78.144.73 205.251.233.122 QM_IDLE        2002    0 ACTIVE
```

Você deve ver uma ou mais linhas contendo um valor de `src` do gateway remoto especificado nos túneis. O `state` deve ser `QM_IDLE` e o `status` deve ser `ACTIVE`. A ausência de uma entrada, ou de qualquer entrada em outro estado, indica que ela não IKE está configurada corretamente.

Para solucionar outros problemas, execute os comandos a seguir para ativar mensagens de log que fornecem informações de diagnóstico.

```
router# term mon
router# debug crypto isakmp
```

Para desativar a depuração, use o comando a seguir.

```
router# no debug crypto isakmp
```

IPsec

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IPsec configurado corretamente.

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
  Crypto map tag: Tunnel1-head-0, local addr 174.78.144.73

  protected vrf: (none)
  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 72.21.209.225 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
    #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.121
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 0xB8357C22(3090512930)

inbound esp sas:
spi: 0x6ADB173(112046451)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4467148/3189)
IV size: 16 bytes
replay detection support: Y replay window size: 128
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xB8357C22(3090512930)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4467148/3189)
IV size: 16 bytes
replay detection support: Y replay window size: 128
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

interface: Tunnel2
Crypto map tag: Tunnel2-head-0, local addr 205.251.233.122

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 72.21.209.193 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
```

```
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.122
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
current outbound spi: 0xF59A3FF6(4120526838)

inbound esp sas:
spi: 0xB6720137(3060924727)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
sa timing: remaining key lifetime (k/sec): (4387273/3492)
IV size: 16 bytes
replay detection support: Y  replay window size: 128
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF59A3FF6(4120526838)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
sa timing: remaining key lifetime (k/sec): (4387273/3492)
IV size: 16 bytes
replay detection support: Y  replay window size: 128
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

Para a interface de cada túnel, você deve ver esp sas de entrada e esp sas de saída. Isso pressupõe que um SA esteja listado (por exemplo, spi: 0x48B456A6), que o status seja ACTIVE e que IPsec esteja configurado corretamente.

Para solucionar outros problemas, use o comando a seguir para ativar a depuração.

```
router# debug crypto ipsec
```

Para desativar a depuração, use o comando a seguir.

```
router# no debug crypto ipsec
```

Túnel

Primeiro, verifique se você implementou as regras de firewall necessárias. Para obter mais informações, consulte [Regras de firewall para seu dispositivo de gateway do cliente](#).

Se as regras de firewall estiverem configuradas corretamente, dê prosseguimento à solução de problemas com o comando a seguir.

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.249.18/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 205.251.233.121
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

Verifique se o protocolo de linha está em execução. Verifique se o endereço IP de origem, a interface de origem e o destino correspondem respectivamente à configuração do túnel para o endereço IP externo do dispositivo de gateway do cliente, à interface e ao endereço IP externo do gateway privado virtual. Verifique se o Tunnel protection through IPsec está presente. Execute o comando em ambas as interfaces do túnel. Para resolver qualquer problema, revise a configuração e verifique as conexões físicas com o dispositivo de gateway do cliente.

Você pode também usar o comando a seguir e substituir 169.254.249.18 pelo endereço IP interno de seu gateway privado virtual.

```
router# ping 169.254.249.18 df-bit size 1410
```

```
Type escape sequence to abort.  
Sending 5, 1410-byte ICMP Echos to 169.254.249.18, timeout is 2 seconds:  
Packet sent with the DF bit set  
!!!!!
```

Você deve ver cinco pontos de exclamação.

Roteamento

Para ver sua tabela de rotas estáticas, use o comando a seguir.

```
router# sh ip route static
```

```
1.0.0.0/8 is variably subnetted  
S      10.0.0.0/16 is directly connected, Tunnel1  
is directly connected, Tunnel2
```

Você deve ver que a rota estática para VPC CIDR atravessar os dois túneis existe. Se não houver, adicione as rotas estáticas conforme indicado a seguir.

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel1 track 100  
router# ip route 10.0.0.0 255.255.0.0 Tunnel2 track 200
```

Verificando o SLA monitor

```
router# show ip sla statistics 100
```

IPSLAs Latest Operation Statistics

```
IPSLA operation id: 100
    Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul 15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

```
router# show ip sla statistics 200
```

IPSLAs Latest Operation Statistics

```
IPSLA operation id: 200
    Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul 15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

O valor de `Number of successes` indica se o SLA monitor foi configurado com sucesso.

Para solucionar outros problemas, revise a configuração.

Solução de problemas de conectividade do dispositivo de gateway do cliente do Juniper JunOS

Ao solucionar problemas de conectividade de um dispositivo de gateway de cliente da Juniper, considere quatro coisas: IKE, IPsec, túnel e BGP. Você pode solucionar essas áreas em qualquer ordem, mas recomendamos que comece com IKE (na parte inferior da pilha de rede) e suba.

IKE

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IKE configurado corretamente.

```
user@router> show security ike security-associations
```

Index	Remote Address	State	Initiator cookie	Responder cookie	Mode
4	72.21.209.225	UP	c4cd953602568b74	0d6d194993328b02	Main
3	72.21.209.193	UP	b8c8fb7dc68d9173	ca7cb0abaedeb4bb	Main

Você deve ver uma ou mais linhas contendo um endereço remoto do gateway remoto especificado nos túneis. O State deve ser UP. A ausência de uma entrada, ou de qualquer entrada em outro estado (como DOWN), é uma indicação de que não IKE está configurada corretamente.

Para solucionar problemas adicionais, ative as opções de IKE rastreamento conforme recomendado no arquivo de configuração de exemplo. Em seguida, execute o comando a seguir para imprimir na tela uma variedade de mensagens de depuração.

```
user@router> monitor start kmd
```

Em um host externo, é possível recuperar o arquivo de log completo com o comando a seguir.

```
scp username@router.hostname:/var/log/kmd
```

IPsec

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IPsec configurado corretamente.

```
user@router> show security ipsec security-associations
```

```
Total active tunnels: 2
ID      Gateway      Port  Algorithm      SPI      Life:sec/kb Mon vsys
<131073 72.21.209.225 500   ESP:aes-128/sha1 df27aae4 326/ unlim - 0
>131073 72.21.209.225 500   ESP:aes-128/sha1 5de29aa1 326/ unlim - 0
<131074 72.21.209.193 500   ESP:aes-128/sha1 dd16c453 300/ unlim - 0
>131074 72.21.209.193 500   ESP:aes-128/sha1 c1e0eb29 300/ unlim - 0
```

Mais especificamente, você deve ver pelo menos duas linhas por endereço de gateway (correspondentes ao gateway remoto). Os operadores maior e menor no início de cada linha (< >) indicam a direção do tráfego para a entrada específica. A saída tem linhas distintas para tráfego de entrada ("<", tráfego do gateway privado virtual para esse dispositivo de gateway do cliente) e tráfego de saída (">").

Para solucionar problemas adicionais, ative as IKE opções de rastreamento (para obter mais informações, consulte a seção anterior sobre). IKE

Túnel

Primeiro, verifique novamente se você implementou as regras de firewall necessárias. Para obter uma lista de regras, consulte [Regras de firewall para seu dispositivo de gateway do cliente](#).

Se as regras de firewall estiverem configuradas corretamente, dê prosseguimento à solução de problemas com o comando a seguir.

```
user@router> show interfaces st0.1
```

```
Logical interface st0.1 (Index 70) (SNMP ifIndex 126)
  Flags: Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel
  Input packets : 8719
  Output packets: 41841
  Security: Zone: Trust
  Allowed host-inbound traffic : bgp ping ssh traceroute
  Protocol inet, MTU: 9192
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
  Destination: 169.254.255.0/30, Local: 169.254.255.2
```

Verifique se Security: Zone está correto e se o endereço Local corresponde ao túnel do dispositivo de gateway do cliente dentro do endereço.

Em seguida, use o comando a seguir e substitua 169.254.255.1 pelo endereço IP interno de seu gateway privado virtual. Os resultados devem ser semelhantes à resposta mostrada aqui.

```
user@router> ping 169.254.255.1 size 1382 do-not-fragment
```

```
PING 169.254.255.1 (169.254.255.1): 1410 data bytes
64 bytes from 169.254.255.1: icmp_seq=0 ttl=64 time=71.080 ms
64 bytes from 169.254.255.1: icmp_seq=1 ttl=64 time=70.585 ms
```

Para solucionar outros problemas, revise a configuração.

BGP

Execute o seguinte comando .

```
user@router> show bgp summary
```

```
Groups: 1 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History  Damp State   Pending
inet.0         2          1          0            0        0      0         0
Peer           AS         InPkt    OutPkt    OutQ   Flaps Last Up/Dwn State|
#Active/Received/Accepted/Damped...
169.254.255.1  7224       9        10        0       0      1:00 1/1/1/0
              0/0/0/0
169.254.255.5  7224       8         9         0       0      56 0/1/1/0
              0/0/0/0
```

Para solucionar outros problemas, use o comando a seguir e substitua 169.254.255.1 pelo endereço IP interno de seu gateway privado virtual.

```
user@router> show bgp neighbor 169.254.255.1
```

```
Peer: 169.254.255.1+179 AS 7224 Local: 169.254.255.2+57175 AS 65000
Type: External State: Established Flags: <ImportEval Sync>
Last State: OpenConfirm Last Event: RecvKeepAlive
Last Error: None
Export: [ EXPORT-DEFAULT ]
Options: <Preference HoldTime PeerAS LocalAS Refresh>
Holdtime: 30 Preference: 170 Local AS: 65000 Local System AS: 0
Number of flaps: 0
Peer ID: 169.254.255.1 Local ID: 10.50.0.10 Active Holdtime: 30
Keepalive Interval: 10 Peer index: 0
BFD: disabled, down
Local Interface: st0.1
NLRI for restart configured on peer: inet-unicast
NLRI advertised by peer: inet-unicast
NLRI for this session: inet-unicast
Peer supports Refresh capability (2)
Restart time configured on the peer: 120
Stale routes from peer are kept for: 300
Restart time requested by this peer: 120
NLRI that peer supports restart for: inet-unicast
NLRI that restart is negotiated for: inet-unicast
NLRI of received end-of-rib markers: inet-unicast
NLRI of all end-of-rib markers sent: inet-unicast
Peer supports 4 byte AS extension (peer-as 7224)
```

```

Table inet.0 Bit: 10000
  RIB State: BGP restart is complete
  Send state: in sync
  Active prefixes:          1
  Received prefixes:       1
  Accepted prefixes:       1
  Suppressed due to damping: 0
  Advertised prefixes:     1
Last traffic (seconds): Received 4   Sent 8   Checked 4
Input messages:  Total 24   Updates 2   Refreshes 0   Octets 505
Output messages: Total 26   Updates 1   Refreshes 0   Octets 582
Output Queue[0]: 0

```

Aqui você deve visualizar `Received prefixes` e `Advertised prefixes` listados com 1. Isso deve estar dentro da seção `Table inet.0`.

Se o State não for `Established`, verifique o `Last State` e o `Last Error` para obter detalhes sobre o que é necessário para corrigir o problema.

Se o BGP peering estiver ativo, verifique se o dispositivo de gateway do cliente está anunciando a rota padrão (0.0.0.0/0) para o VPC

```

user@router> show route advertising-protocol bgp 169.254.255.1

```

```

inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix          Nexthop          MED    Lclpref    AS path
* 0.0.0.0/0      Self

```

Além disso, verifique se você está recebendo o prefixo que corresponde ao seu VPC do gateway privado virtual.

```

user@router> show route receive-protocol bgp 169.254.255.1

```

```

inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix          Nexthop          MED    Lclpref    AS path
* 10.110.0.0/16  169.254.255.1   100

```

Solução de problemas de conectividade de gateway do cliente do Juniper ScreenOS

Ao solucionar problemas de conectividade de um dispositivo de gateway de cliente baseado em ScreenOS da Juniper, considere quatro coisas: IKE, IPsec, túnel e BGP. Você pode solucionar essas áreas em qualquer ordem, mas recomendamos que comece com IKE (na parte inferior da pilha de rede) e suba.

IKE e IPsec

Use o seguinte comando. A resposta mostra um dispositivo de gateway do cliente IKE configurado corretamente.

```
ssg5-serial-> get sa
```

```
total configured sa: 2
HEX ID      Gateway          Port Algorithm      SPI          Life:sec kb Sta  PID vsys
00000002<  72.21.209.225  500 esp:a128/sha1 80041ca4  3385 unlim A/-  -1 0
00000002>  72.21.209.225  500 esp:a128/sha1 8cdd274a  3385 unlim A/-  -1 0
00000001<  72.21.209.193  500 esp:a128/sha1 ecf0bec7  3580 unlim A/-  -1 0
00000001>  72.21.209.193  500 esp:a128/sha1 14bf7894  3580 unlim A/-  -1 0
```

Você deve ver uma ou mais linhas contendo um endereço remoto do gateway remoto especificado nos túneis. O valor Sta deve ser A/- e o SPI deve ser um número hexadecimal diferente de 00000000. Entradas em outros estados indicam que não IKE está configurado corretamente.

Para solucionar problemas adicionais, ative as opções de IKE rastreamento (conforme recomendado no arquivo de configuração de exemplo).

Túnel

Primeiro, verifique novamente se você implementou as regras de firewall necessárias. Para obter uma lista de regras, consulte [Regras de firewall para seu dispositivo de gateway do cliente](#).

Se as regras de firewall estiverem configuradas corretamente, dê prosseguimento à solução de problemas com o comando a seguir.

```
ssg5-serial-> get interface tunnel1.1
```

```
Interface tunnel.1:
description tunnel.1
number 20, if_info 1768, if_index 1, mode route
link ready
vsys Root, zone Trust, vr trust-vr
admin mtu 1500, operating mtu 1500, default mtu 1500
*ip 169.254.255.2/30
*manage ip 169.254.255.2
route-deny disable
bound vpn:
  IPSEC-1
```

```
Next-Hop Tunnel Binding table
Flag Status Next-Hop(IP)   tunnel-id  VPN
```

```
pmtu-v4 disabled
ping disabled, telnet disabled, SSH disabled, SNMP disabled
web disabled, ident-reset disabled, SSL disabled
```

```
OSPF disabled  BGP enabled  RIP disabled  RIPng disabled  mtrace disabled
PIM: not configured  IGMP not configured
NHRP disabled
bandwidth: physical 0kbps, configured egress [gbw 0kbps mbw 0kbps]
             configured ingress mbw 0kbps, current bw 0kbps
             total allocated gbw 0kbps
```

Verifique se `link:ready` está presente e se o endereço IP corresponde ao endereço interno do túnel do dispositivo de gateway do cliente.

Em seguida, use o comando a seguir e substitua `169.254.255.1` pelo endereço IP interno de seu gateway privado virtual. Os resultados devem ser semelhantes à resposta mostrada aqui.

```
ssg5-serial-> ping 169.254.255.1
```

```
Type escape sequence to abort
```

```
Sending 5, 100-byte ICMP Echos to 169.254.255.1, timeout is 1 seconds
```

```
!!!!
```

```
Success Rate is 100 percent (5/5), round-trip time min/avg/max=32/32/33 ms
```

Para solucionar outros problemas, revise a configuração.

BGP

Execute o seguinte comando .

```
ssg5-serial-> get vrouter trust-vr protocol bgp neighbor
```

Peer AS	Remote IP	Local IP	Wt	Status	State	ConnID	Up/Down
7224	169.254.255.1	169.254.255.2	100	Enabled	ESTABLISH	10	00:01:01
7224	169.254.255.5	169.254.255.6	100	Enabled	ESTABLISH	11	00:00:59

O estado de ambos os BGP pares deve ser ESTABLISH, o que significa que a BGP conexão com o gateway privado virtual está ativa.

Para solucionar outros problemas, use o comando a seguir e substitua 169.254.255.1 pelo endereço IP interno de seu gateway privado virtual.

```
ssg5-serial-> get vr trust-vr prot bgp neigh 169.254.255.1
```

```
peer: 169.254.255.1, remote AS: 7224, admin status: enable
type: EBGp, multihop: 0(disable), MED: node default(0)
connection state: ESTABLISH, connection id: 18 retry interval: node default(120s), cur
  retry time 15s
configured hold time: node default(90s), configured keepalive: node default(30s)
configured adv-interval: default(30s)
designated local IP: n/a
local IP address/port: 169.254.255.2/13946, remote IP address/port: 169.254.255.1/179
router ID of peer: 169.254.255.1, remote AS: 7224
negotiated hold time: 30s, negotiated keepalive interval: 10s
route map in name: , route map out name:
weight: 100 (default)
self as next hop: disable
send default route to peer: disable
ignore default route from peer: disable
send community path attribute: no
reflector client: no
Neighbor Capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast: advertised and received
force reconnect is disable
total messages to peer: 106, from peer: 106
```

```
update messages to peer: 6, from peer: 4
Tx queue length 0, Tx queue HWM: 1
route-refresh messages to peer: 0, from peer: 0
last reset 00:05:33 ago, due to BGP send Notification(Hold Timer Expired)(code 4 :
  subcode 0)
number of total successful connections: 4
connected: 2 minutes 6 seconds
Elapsed time since last update: 2 minutes 6 seconds
```

Se o BGP peering estiver ativo, verifique se o dispositivo de gateway do cliente está anunciando a rota padrão (0.0.0.0/0) para o VPC. Esse comando aplica-se ao ScreenOS versão 6.2.0 e superior.

```
s5g5-serial-> get vr trust-vr protocol bgp rib neighbor 169.254.255.1 advertised
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
      Prefix          Nexthop    Wt  Pref  Med Orig   AS-Path
-----
>i      0.0.0.0/0      0.0.0.0 32768  100   0  IGP
Total IPv4 routes advertised: 1
```

Além disso, verifique se você está recebendo o prefixo que corresponde ao seu VPC do gateway privado virtual. Esse comando aplica-se ao ScreenOS versão 6.2.0 e superior.

```
s5g5-serial-> get vr trust-vr protocol bgp rib neighbor 169.254.255.1 received
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
      Prefix          Nexthop    Wt  Pref  Med Orig   AS-Path
-----
>e*    10.0.0.0/16     169.254.255.1 100  100  100  IGP   7224
Total IPv4 routes received: 1
```

Solução de problemas de conectividade do dispositivo de gateway do cliente da Yamaha

Ao solucionar problemas de conectividade de um dispositivo Yamaha Customer Gateway, considere quatro coisas: IKE, IPsec, túnel e BGP. Você pode solucionar essas áreas em qualquer ordem, mas recomendamos que comece com IKE (na parte inferior da pilha de rede) e suba.

Note

A `proxy ID` configuração usada na fase 2 do IKE está desativada por padrão no roteador Yamaha. Isso pode causar problemas na conexão com o site a site. VPN Se o não `proxy ID` estiver configurado em seu roteador, consulte o exemplo de arquivo AWS de configuração fornecido para que a Yamaha defina corretamente.

IKE

Execute o seguinte comando . A resposta mostra um dispositivo de gateway do cliente IKE configurado corretamente.

```
# show ipsec sa gateway 1
```

sgw	flags	local-id	remote-id	# of sa
1	U K	YOUR_LOCAL_NETWORK_ADDRESS	72.21.209.225	i:2 s:1 r:1

Você deve ver uma linha contendo um valor `remote-id` do gateway remoto especificado nos túneis. Você pode listar todas as associações de segurança (SAs) omitindo o número do túnel.

Para solucionar problemas adicionais, execute os comandos a seguir para ativar mensagens de log de DEBUG nível que forneçam informações de diagnóstico.

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

Para cancelar os itens registrados, execute o comando a seguir.

```
# no ipsec ike log
# no syslog debug on
```

IPsec

Execute o seguinte comando . A resposta mostra um dispositivo de gateway do cliente IPsec configurado corretamente.

```
# show ipsec sa gateway 1 detail
```

```

SA[1] Duration: 10675s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit

SPI: 6b ce fd 8a d5 30 9b 02 0c f3 87 52 4a 87 6e 77
Key: ** ** ** ** ** (confidential) ** ** ** ** **
-----

SA[2] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: send
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: a6 67 47 47
Key: ** ** ** ** ** (confidential) ** ** ** ** **
-----

SA[3] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: receive
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: 6b 98 69 2b
Key: ** ** ** ** ** (confidential) ** ** ** ** **
-----

SA[4] Duration: 10681s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit
SPI: e8 45 55 38 90 45 3f 67 a8 74 ca 71 ba bb 75 ee
Key: ** ** ** ** ** (confidential) ** ** ** ** **
-----

```

Para a interface de cada túnel, você deve ver `receive sas` e `send sas`.

Para solucionar outros problemas, use o comando a seguir para ativar a depuração.

```

# syslog debug on
# ipsec ike log message-info payload-info key-info

```

Execute o comando a seguir para desabilitar a depuração.

```
# no ipsec ike log
# no syslog debug on
```

Túnel

Primeiro, verifique se você implementou as regras de firewall necessárias. Para obter uma lista de regras, consulte [Regras de firewall para seu dispositivo de gateway do cliente](#).

Se as regras de firewall estiverem configuradas corretamente, dê prosseguimento à solução de problemas com o comando a seguir.

```
# show status tunnel 1
```

```
TUNNEL[1]:
Description:
  Interface type: IPsec
  Current status is Online.
  from 2011/08/15 18:19:45.
  5 hours 7 minutes 58 seconds connection.
  Received:      (IPv4) 3933 packets [244941 octets]
                 (IPv6) 0 packet [0 octet]
  Transmitted:  (IPv4) 3933 packets [241407 octets]
                 (IPv6) 0 packet [0 octet]
```

Certifique-se de que o `current status` valor esteja on-line e `Interface type` pronto IPsec. Lembre-se de executar o comando em ambas as interfaces do túnel. Para solucionar qualquer problema aqui, revise a configuração.

BGP

Execute o seguinte comando .

```
# show status bgp neighbor
```

```
BGP neighbor is 169.254.255.1, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
```

```

Received 0 messages, 0 notifications, 0 in queue
Sent 0 messages, 0 notifications, 0 in queue
Connection established 0; dropped 0
Last reset never
Local host: unspecified
Foreign host: 169.254.255.1, Foreign port: 0

BGP neighbor is 169.254.255.5, remote AS 7224, local AS 65000, external link
BGP version 0, remote router ID 0.0.0.0
BGP state = Active
Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
Received 0 messages, 0 notifications, 0 in queue
Sent 0 messages, 0 notifications, 0 in queue
Connection established 0; dropped 0
Last reset never
Local host: unspecified
Foreign host: 169.254.255.5, Foreign port:

```

Ambos os vizinhos deve ser listados. Para cada um, você deve ver um valor BGP state de Active.

Se o BGP peering estiver ativo, verifique se o dispositivo de gateway do cliente está anunciando a rota padrão (0.0.0.0/0) para o VPC

```
# show status bgp neighbor 169.254.255.1 advertised-routes
```

```

Total routes: 1
*: valid route
  Network          Next Hop          Metric LocPrf Path
* default          0.0.0.0           0       IGP

```

Além disso, verifique se você está recebendo o prefixo que corresponde ao seu VPC do gateway privado virtual.

```
# show ip route
```

Destination	Gateway	Interface	Kind	Additional Info.
default	***.***.***.***	LAN3(DHCP)	static	
10.0.0.0/16	169.254.255.1	TUNNEL[1]	BGP	path=10124

Trabalhar com o Site-to-Site VPN

É possível trabalhar com recursos do Site-to-Site VPN usando o console da Amazon VPC ou a CLI da AWS CLI.

Conteúdo

- [Crie um anexo VPN Site-to-Site para Cloud WAN AWS](#)
- [Criar um anexo de VPN do gateway de trânsito](#)
- [Testar uma conexão do Site-to-Site VPN](#)
- [Excluir uma conexão do Site-to-Site VPN](#)
- [Modificar o gateway de destino da conexão do Site-to-Site VPN](#)
- [Modificar as opções de conexão do Site-to-Site VPN](#)
- [Modificar opções de túnel do Site-to-Site VPN](#)
- [Editar rotas estáticas para uma conexão do Site-to-Site VPN](#)
- [Alterar o gateway do cliente para uma conexão do Site-to-Site VPN](#)
- [Substituir as credenciais comprometidas para a conexão do Site-to-Site VPN](#)
- [Alternar os certificados de endpoint do túnel do Site-to-Site VPN](#)
- [VPN IP privada com AWS Direct Connect](#)

Crie um anexo VPN Site-to-Site para Cloud WAN AWS

Siga o procedimento abaixo para criar um anexo VPN Site-to-Site para Cloud WAN. AWS

Para criar um anexo VPN para o AWS Cloud WAN usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Escolha Create VPN Connection (Criar conexão VPN).
4. (Opcional) Em Etiqueta de nome, insira um nome para a conexão. Ao fazer isso, é criada uma tag com a chave Name e o valor especificado.
5. Para Target Gateway Type (Tipo de gateway de destino), escolha Not Associated (Não associado).
6. Em Customer Gateway (Gateway do cliente), execute um dos procedimentos a seguir:

- Para usar um gateway do cliente existente, escolha Existente e selecione o gateway do cliente.
 - Para criar um gateway do cliente, escolha New (Novo). Para IP Address (Endereço IP), insira um endereço IP público estático. Para Certificate ARN (ARN do certificado), escolha o ARN do certificado privado (se estiver usando autenticação baseada em certificado). Para BGP ASN, informe o Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) do gateway do cliente. Para ter mais informações, consulte [Opções de gateway do cliente](#).
7. Em Opções de roteamento, escolha entre Dinâmico ou Estático.
 8. Em Versão IP de túnel interno, escolha IPv4 ou IPv6.
 9. (Opcional) Para Enable Acceleration (Habilitar aceleração), marque a caixa de seleção para habilitar a aceleração. Para ter mais informações, consulte [Conexões VPN aceleradas](#).

Se você habilitar a aceleração, criaremos dois aceleradores que são usados pela sua conexão VPN. Aplicam-se cobranças adicionais de .

10. (Opcional) Para Local IPv4 Network CIDR (CIDR de rede IPv4 local), especifique o intervalo CIDR IPv4 no lado do gateway do cliente (no local) que tem permissão para se comunicar pelos túneis da VPN. O padrão é `0.0.0.0/0`.

Para CIDR de rede IPv4 remota, especifique o intervalo de CIDR IPv4 no AWS lado que tem permissão para se comunicar pelos túneis VPN. O padrão é `0.0.0.0/0`.

Se você especificou IPv6 para túnel dentro da versão IP, especifique os intervalos de CIDR IPv6 no lado e AWS no lado do gateway do cliente que podem se comunicar pelos túneis VPN. O padrão para ambos os intervalos é `::/0`.

11. (Opcional) Em Opções de túnel, é possível especificar as seguintes informações para cada túnel:
 - Um bloco CIDR do IPv4 de tamanho /30 do intervalo `169.254.0.0/16` para os endereços IPv4 do túnel interno.
 - Se você especificou IPv6 em Versão IP de túnel interno, um bloco CIDR do IPv6 /126 do intervalo `fd00::/8` para os endereços IPv6 do túnel interno.
 - A chave pré-compartilhada do IKE (PSK). As seguintes versões são compatíveis: IKEv1 ou IKEv2.
 - Para editar as opções avançadas do túnel, escolha Editar opções de túnel. Para ter mais informações, consulte [Opções de túnel VPN](#).

12. Escolha Create VPN Connection (Criar conexão VPN).

Como criar uma conexão de VPN de local a local usando a linha de comando ou a API

- [CreateVpnConnection](#)(API de consulta do Amazon EC2)
- [create-vpn-connection](#) (AWS CLI)

Criar um anexo de VPN do gateway de trânsito

Para criar um anexo de VPN em um gateway de trânsito, especifique o gateway de trânsito e o gateway do cliente. O gateway de trânsito precisará ser criado antes de seguir este procedimento. Para obter mais informações sobre como criar um gateway de trânsito, consulte [Gateways de trânsito](#) em Gateways de trânsito da Amazon VPC.

Para criar um anexo de VPN em um gateway de trânsito usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Escolha Create VPN Connection (Criar conexão VPN).
4. (Opcional) Em Etiqueta de nome, insira um nome para a conexão. Ao fazer isso, é criada uma tag com a chave Name e o valor especificado.
5. Em Tipo de gateway de destino, selecione Gateway de trânsito e escolha o gateway de trânsito.
6. Em Customer Gateway (Gateway do cliente), execute um dos procedimentos a seguir:
 - Para usar um gateway do cliente existente, escolha Existente e selecione o gateway do cliente.

Se o gateway do cliente estiver atrás de um dispositivo de tradução de endereço de rede (NAT), que esteja habilitado para NAT traversal (NAT-T), use o endereço IP público do dispositivo NAT e ajuste as regras de firewall para desbloquear a porta UDP 4500.

- Para criar um gateway do cliente, escolha New (Novo). Para IP Address (Endereço IP), insira um endereço IP público estático. Para Certificate ARN (ARN do certificado), escolha o ARN do certificado privado (se estiver usando autenticação baseada em certificado). Para BGP ASN, informe o Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) do gateway do cliente. Para ter mais informações, consulte [Opções de gateway do cliente](#).

7. Em Opções de roteamento, escolha entre Dinâmico ou Estático.
8. Em Versão IP de túnel interno, especifique se os túneis VPN são compatíveis com tráfego IPv4 ou IPv6. O tráfego IPv6 só é compatível com conexões VPN em um gateway de trânsito.
9. (Opcional) Para Enable Acceleration (Habilitar aceleração), marque a caixa de seleção para habilitar a aceleração. Para ter mais informações, consulte [Conexões VPN aceleradas](#).

Se você habilitar a aceleração, criaremos dois aceleradores que são usados pela sua conexão VPN. Aplicam-se cobranças adicionais de .

10. (Opcional) Para Local IPv4 Network CIDR (CIDR de rede IPv4 local), especifique o intervalo CIDR IPv4 no lado do gateway do cliente (no local) que tem permissão para se comunicar pelos túneis da VPN. O padrão é `0.0.0.0/0`.

Para CIDR de rede IPv4 remota, especifique o intervalo de CIDR IPv4 no AWS lado que tem permissão para se comunicar pelos túneis VPN. O padrão é `0.0.0.0/0`.

Se você especificou IPv6 para túnel dentro da versão IP, especifique os intervalos de CIDR IPv6 no lado e AWS no lado do gateway do cliente que podem se comunicar pelos túneis VPN. O padrão para ambos os intervalos é `::/0`.

11. (Opcional) Em Opções de túnel, é possível especificar as seguintes informações para cada túnel:
 - Um bloco CIDR do IPv4 de tamanho /30 do intervalo `169.254.0.0/16` para os endereços IPv4 do túnel interno.
 - Se você especificou IPv6 em Versão IP de túnel interno, um bloco CIDR do IPv6 /126 do intervalo `fd00::/8` para os endereços IPv6 do túnel interno.
 - A chave pré-compartilhada do IKE (PSK). As seguintes versões são compatíveis: IKEv1 ou IKEv2.
 - Para editar as opções avançadas do túnel, escolha Editar opções de túnel. Para ter mais informações, consulte [Opções de túnel VPN](#).
12. Escolha Create VPN Connection (Criar conexão VPN).

Para criar um anexo VPN usando o AWS CLI

Use o [create-vpn-connection](#) comando e especifique o ID do gateway de trânsito para a `--transit-gateway-id` opção.

Testar uma conexão do Site-to-Site VPN

Depois de criar a AWS Site-to-Site VPN conexão e configurar o gateway do cliente, você pode iniciar uma instância e testar a conexão fazendo ping na instância.

Antes de começar, certifique-se do seguinte:

- Use uma AMI que responda a solicitações de ping. Recomendamos que você use uma das Amazon Linux AMIs.
- Configure qualquer grupo de segurança ou network ACL na VPC que filtre o tráfego para a instância para permitir o tráfego ICMP de entrada e de saída. Isso permite que a instância receba solicitações ping.
- Caso as instâncias executem o Windows Server, conecte-se à instância e permita o ICMPv4 de entrada no firewall do Windows para que o ping seja executado na instância.
- (Roteamento estático) Certifique-se de que o dispositivo de gateway do cliente tenha uma rota estática para a VPC e que a conexão VPN tenha uma rota estática para que o tráfego possa retornar ao dispositivo de gateway do cliente.
- (Roteamento dinâmico) Certifique-se de que o status BGP no dispositivo de gateway do cliente esteja estabelecido. Leva cerca de 30 segundos para que a sessão de emparelhamento de BGP seja estabelecida. Verifique se as rotas estão anunciadas com BGP corretamente e à mostra na tabela de rotas da sub-rede de modo que o tráfego possa voltar ao gateway do cliente. Verifique se os dois túneis estão configurados com roteamento BGP.
- Verifique se você configurou o roteamento nas tabelas de rotas da sub-rede para a conexão VPN.

Como testar a conectividade

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel, escolha Executar instância.
3. (Opcional) Em Nome, insira um nome descritivo para a instância.
4. Em Imagens de aplicações e sistemas operacionais (imagem de máquina da Amazon), escolha Início rápido e, depois, escolha o sistema operacional da instância.
5. Em Nome do par de chaves, escolha um par de chaves existente ou crie outro.
6. Em Configurações de rede, escolha Selecionar grupo de segurança existente e, depois, escolha o grupo de segurança que você configurou.
7. No painel Resumo painel, escolha Iniciar instância.

- Depois que a instância estiver em execução, obtenha o endereço IP privado (por exemplo, 10.0.0.4). O console do Amazon EC2 exibe o endereço como parte dos detalhes da instância.
- Em um computador na rede que esteja por trás do gateway do cliente, use o comando ping com o endereço IP privado da instância.

```
ping 10.0.0.4
```

Uma resposta bem-sucedida assemelha-se ao seguinte.

```
Pinging 10.0.0.4 with 32 bytes of data:  
  
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128  
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128  
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128  
  
Ping statistics for 10.0.0.4:  
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),  
  
Approximate round trip times in milliseconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Para testar o failover de túnel, é possível desabilitar temporariamente um dos túneis no dispositivo de gateway do cliente e repetir esta etapa. Não é possível desabilitar um túnel no lado da AWS da conexão VPN.

- Para testar a conexão com sua rede local, você pode usar SSH ou RDP para se conectar à sua instância a partir da sua rede. AWS Depois, é possível executar o comando ping com o endereço IP privado de outro computador na rede, para verificar se ambos os lados da conexão podem iniciar e receber solicitações.

Para obter mais informações sobre como se conectar a uma instância Linux, consulte [Conecte-se à sua instância Linux](#) no Guia do usuário do Amazon EC2. Para obter mais informações sobre como se conectar a uma instância do Windows, consulte [Conecte-se à sua instância do Windows](#) no Guia do usuário do Amazon EC2.

Excluir uma conexão do Site-to-Site VPN

Se você não precisar mais de uma AWS Site-to-Site VPN conexão, poderá excluí-la. Quando você exclui uma conexão do Site-to-Site VPN, não excluimos o gateway do cliente ou o gateway privado

virtual associado à conexão do Site-to-Site VPN. Se você não precisar mais do gateway do cliente e do gateway privado virtual, poderá excluí-los.

Warning

Se você excluir a conexão do Site-to-Site VPN e criar outra, será necessário baixar um novo arquivo de configuração e reconfigurar o dispositivo de gateway do cliente.

Tarefas

- [Excluir uma conexão VPN](#)
- [Excluir um gateway do cliente](#)
- [Desanexar e excluir um gateway privado virtual](#)

Excluir uma conexão VPN

Depois de excluir a conexão do Site-to-Site VPN, ela permanece visível por um curto período com um estado de `deleted` e, depois, a entrada é removida automaticamente.

Para excluir uma conexão VPN usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão VPN e escolha Ações, Excluir conexão VPN.
4. Quando a confirmação for solicitada, insira **delete** e escolha Excluir.

Para excluir uma conexão VPN usando a linha de comando ou a API

- [DeleteVpnConnection](#)(API de consulta do Amazon EC2)
- [delete-vpn-connection](#) (AWS CLI)
- [Remove-EC2VpnConnection](#) (AWS Tools for Windows PowerShell)

Excluir um gateway do cliente

Caso não precise mais de um gateway do cliente, é possível excluí-lo. Não é possível excluir um gateway do cliente que está sendo usado em uma conexão do Site-to-Site VPN.

Para excluir um gateway do cliente usando o console

1. No painel de navegação, escolha Gateways do cliente.
2. Selecione o gateway do cliente e escolha Ações, Excluir gateway do cliente.
3. Quando a confirmação for solicitada, insira **delete** e escolha Excluir.

Para excluir um gateway do cliente usando a linha de comando ou a API

- [DeleteCustomerGateway](#)(API de consulta do Amazon EC2)
- [delete-customer-gateway](#) (AWS CLI)
- [Remove-EC2CustomerGateway](#) (AWS Tools for Windows PowerShell)

Desanexar e excluir um gateway privado virtual

Caso não precise mais de um gateway privado virtual para a VPC, desanexe-o dela.

Para desanexar um gateway privado virtual usando o console

1. No painel de navegação, escolha Gateways privados virtuais.
2. Selecione o gateway privado virtual e escolha Actions, Detach from VPC.
3. Escolha Desanexar gateway privado virtual.

Caso não precise mais de um gateway privado virtual desanexado, exclua-o. Não é possível excluir um gateway privado virtual que ainda esteja anexado à VPC. Depois de excluir o gateway privado virtual, ele permanecerá visível por um breve período com um estado de `deleted` e, em seguida, a entrada é removida automaticamente.

Para excluir um gateway privado virtual usando o console

1. No painel de navegação, escolha Gateways privados virtuais.
2. Selecione o gateway privado virtual e escolha Ações, Excluir gateway privado virtual.
3. Quando a confirmação for solicitada, insira **delete** e escolha Excluir.

Para desanexar um gateway privado virtual usando a linha de comando ou a API

- [DetachVpnGateway](#)(API de consulta do Amazon EC2)

- [detach-vpn-gateway](#) (AWS CLI)
- [Dismount-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

Para excluir um gateway privado virtual usando a linha de comando ou a API

- [DeleteVpnGateway](#)(API de consulta do Amazon EC2)
- [delete-vpn-gateway](#) (AWS CLI)
- [Remove-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

Modificar o gateway de destino da conexão do Site-to-Site VPN

Você pode modificar o gateway de destino de uma AWS Site-to-Site VPN conexão. As seguintes opções de migração estão disponíveis:

- Um gateway privado virtual existente para um gateway de trânsito
- Um gateway privado virtual existente para outro gateway privado virtual
- Um gateway de trânsito existente para outro gateway de trânsito
- Um gateway de trânsito existente para um gateway privado virtual

Depois de modificar o gateway de destino, a conexão de VPN de local a local ficará indisponível durante um breve período enquanto provisionamos os novos endpoints.

As tarefas a seguir ajudam você a concluir a migração para um novo gateway.

Tarefas

- [Etapa 1: Criar o gateway de destino](#)
- [Etapa 2: excluir as rotas estáticas \(condicional\)](#)
- [Etapa 3: Migrar para um novo gateway](#)
- [Etapa 4: Atualizar tabelas de rotas da VPC](#)
- [Etapa 5: Atualizar o roteamento do gateway de destino \(condicional\)](#)
- [Etapa 6: atualizar o ASN do gateway do cliente \(condicional\)](#)

Etapa 1: Criar o gateway de destino

Antes de realizar a migração para o novo gateway, é necessário configurá-lo. Para obter informações sobre como adicionar um gateway privado virtual, consulte [the section called “Criar um gateway privado virtual”](#). Para obter mais informações sobre como adicionar um gateway de trânsito, consulte [Criar um gateway de trânsito](#) em Gateways de trânsito da Amazon VPC.

Se o novo gateway de destino for um gateway de trânsito, conecte as VPCs ao gateway de trânsito. Para obter informações sobre anexos de VPC, consulte [Anexos do gateway de trânsito de uma VPC](#) em Gateways de trânsito da Amazon VPC.

Ao modificar o destino de um gateway privado virtual para um gateway de trânsito, você pode, opcionalmente, definir o ASN do gateway de trânsito para ter o mesmo valor que o ASN do gateway privado virtual. Se você optar por ter um ASN diferente, deverá definir o ASN no dispositivo gateway do cliente como o ASN do gateway de trânsito. Para ter mais informações, consulte [the section called “Etapa 6: atualizar o ASN do gateway do cliente \(condicional\)”](#).

Etapa 2: excluir as rotas estáticas (condicional)

Esta etapa é necessária quando você migra de um gateway privado virtual com rotas estáticas para um gateway de trânsito.

É necessário excluir as rotas estáticas antes de migrar para o novo gateway.

Tip

Mantenha uma cópia da rota estática antes de excluí-la. Você precisará adicionar novamente essas rotas ao gateway de trânsito depois que a migração da conexão VPN for concluída.

Para excluir uma rota da tabela

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Route Tables (Tabelas de rotas) e selecione a tabela de rotas.
3. Na guia Rotas, escolha Editar rotas.
4. Escolha Remove para a rota estática do gateway privado virtual.
5. Escolha Salvar alterações.

Etapa 3: Migrar para um novo gateway

Como alterar o gateway de destino

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão VPN e escolha Ações, Modificar conexão VPN.
4. Em Tipo de destino, escolha o tipo de gateway.
 - a. Se o novo gateway de destino for um gateway privado virtual, escolha Gateway VPN.
 - b. Se o novo gateway de destino for um gateway de trânsito, escolha Gateway de trânsito.
5. Escolha Salvar alterações.

Como modificar uma conexão de VPN de local a local usando a linha de comando ou a API

- [ModifyVpnConnection](#) (API de consulta do Amazon EC2)
- [modify-vpn-connection](#) (AWS CLI)

Etapa 4: Atualizar tabelas de rotas da VPC

Depois de migrar para o novo gateway, talvez seja necessário modificar a tabela de rotas da VPC. Para obter mais informações, consulte [Tabelas de rotas](#) no Guia do usuário da Amazon VPC.

A tabela a seguir fornece informações sobre as atualizações da tabela de rotas da VPC a serem feitas após modificar o destino do gateway VPN.

Gateway existente	Novo gateway	Alteração de tabela de rotas da VPC
Gateway privado virtual com rotas propagadas	Transit gateway	Adicione uma rota que contenha o ID do gateway de trânsito.
Gateway privado virtual com rotas propagadas	Gateway privado virtual com rotas propagadas	Nenhuma ação é necessária.

Gateway existente	Novo gateway	Alteração de tabela de rotas da VPC
Gateway privado virtual com rotas propagadas	Gateway privado virtual com rota estática	Adicione uma rota que contenha o ID do novo gateway privado virtual.
Gateway privado virtual com rotas estáticas	Transit gateway	Atualize a rota que contém o ID do gateway privado virtual para o ID do gateway de trânsito.
Gateway privado virtual com rotas estáticas	Gateway privado virtual com rotas estáticas	Atualize a rota que contém o ID do gateway privado virtual para o ID do novo gateway privado virtual.
Gateway privado virtual com rotas estáticas	Gateway privado virtual com rotas propagadas	Exclua a rota que contém o ID do gateway privado virtual.
Transit gateway	Gateway privado virtual com rotas estáticas	Atualize a rota que contém o ID do gateway de trânsito para o ID do gateway privado virtual.
Transit gateway	Gateway privado virtual com rotas propagadas	Exclua a rota que contém o ID de gateway de trânsito.
Transit gateway	Transit gateway	Atualize a rota que contém o ID do gateway de trânsito para o ID do novo gateway de trânsito.

Etapa 5: Atualizar o roteamento do gateway de destino (condicional)

Quando o novo gateway for um gateway de trânsito, modifique a tabela de rotas para permitir o tráfego entre a VPC e a VPN de local a local. Para obter mais informações, consulte [Tabelas de rota de Transit gateway](#) em Amazon VPC Transit Gateway.

Se você tiver excluído rotas estáticas de VPN, deverá adicionar essas rotas estáticas à tabela de rotas do gateway de trânsito.

Ao contrário de um gateway privado virtual, um gateway de trânsito define o mesmo valor para o discriminador de várias saídas (MED) em todos os túneis em um anexo da VPN. Se você está migrando de um gateway privado virtual para um gateway de trânsito e baseou-se no valor MED para seleção de túnel, recomendamos que faça alterações de roteamento para evitar problemas de conexão. Por exemplo, você pode anunciar rotas mais específicas em seu gateway de trânsito. Para ter mais informações, consulte [Tabelas de rotas e prioridade de VPN rotas](#).

Etapa 6: atualizar o ASN do gateway do cliente (condicional)

Quando o novo gateway tiver um ASN diferente do gateway antigo, atualize o ASN no dispositivo de gateway do cliente para apontar para o novo ASN. Consulte [Opções de gateway do cliente para a conexão de VPN de local a local](#) para obter mais informações.

Modificar as opções de conexão do Site-to-Site VPN

Você pode modificar as opções de conexão para sua conexão do Site-to-Site VPN. É possível modificar as opções a seguir:

- Os intervalos CIDR IPv4 no lado local (gateway do cliente) e no lado remoto (AWS) da conexão VPN que pode se comunicar pelos túneis da VPN. O padrão é `0.0.0.0/0` para ambos os intervalos.
- Os intervalos CIDR IPv6 no lado local (gateway do cliente) e no lado remoto (AWS) da conexão VPN que pode se comunicar pelos túneis da VPN. O padrão é `::/0` para ambos os intervalos.

Quando você modifica as opções de conexão VPN, os endereços IP do endpoint VPN na AWS lateral não são alterados e as opções de túnel não mudam. A conexão VPN ficará temporariamente indisponível enquanto a conexão VPN for atualizada.

Como modificar as opções de conexão VPN usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão VPN e escolha Ações, Modificar opções de conexão VPN.
4. Insira novos intervalos de CIDR, conforme necessário.

5. Escolha Salvar alterações.

Como modificar as opções de conexão VPN usando a linha de comando ou a API

- [modify-vpn-connection-options](#) (AWS CLI)
- [ModifyVpnConnectionOptions](#)(API de consulta do Amazon EC2)

Modificar opções de túnel do Site-to-Site VPN

Você pode modificar as opções dos túneis VPN em sua conexão do Site-to-Site VPN. É possível modificar um túnel VPN de cada vez.

Important

Quando você modifica um túnel VPN, a conectividade pelo túnel é interrompida por até vários minutos. Planeje o tempo de inatividade esperado.

Como modificar as opções de túnel VPN usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão do Site-to-Site VPN e escolha Ações, Modificar opções de túnel VPN.
4. Em Endereço IP externo do túnel VPN, escolha o IP do endpoint do túnel VPN.
5. Escolha ou insira novos valores para as opções de túnel, conforme necessário. Para ter mais informações, consulte [Opções de túnel VPN](#).
6. Escolha Salvar alterações.

Como modificar as opções de túnel VPN usando a linha de comando ou a API

- (AWS CLI) Use [describe-vpn-connections](#) para visualizar as opções de túnel atuais e [modify-vpn-tunnel-options](#) para modificar as opções de túnel.
- (Amazon EC2 Query API) Use [DescribeVpnConnections](#) para visualizar as opções de túnel atuais e [ModifyVpnTunnelOptions](#) para modificar as opções de túnel.

Editar rotas estáticas para uma conexão do Site-to-Site VPN

Para uma conexão do Site-to-Site VPN em um gateway privado virtual configurado para roteamento estático, você pode adicionar ou remover as rotas estáticas da configuração de VPN.

Como adicionar ou remover uma rota estática usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão VPN.
4. Escolha Editar rotas estáticas.
5. Adicione ou remova rotas, conforme necessário.
6. Escolha Salvar alterações.
7. Se a propagação da rota não estiver habilitada para a tabela de rotas, será preciso atualizar as rotas manualmente na tabela de rotas para, assim, refletir os prefixos IP estáticos atualizados na conexão VPN. Para ter mais informações, consulte [\(Gateway privado virtual\) Habilitar a propagação de rotas na tabela de rotas](#).
8. Para uma conexão VPN em um gateway de trânsito, você adiciona, modifica ou remove as rotas estáticas na tabela de rotas do gateway de trânsito. Para obter mais informações, consulte [Tabelas de rota de Transit gateway](#) em Amazon VPC Transit Gateway.

Para adicionar uma rota estática usando a linha de comando ou a API

- [CreateVpnConnectionRoute](#)(API de consulta do Amazon EC2)
- [create-vpn-connection-route](#) (AWS CLI)
- [New-EC2VpnConnectionRoute](#) (AWS Tools for Windows PowerShell)

Para excluir uma rota estática usando a linha de comando ou a API

- [DeleteVpnConnectionRoute](#)(API de consulta do Amazon EC2)
- [delete-vpn-connection-route](#) (AWS CLI)
- [Remove-EC2VpnConnectionRoute](#) (AWS Tools for Windows PowerShell)

Alterar o gateway do cliente para uma conexão do Site-to-Site VPN

Você pode alterar o gateway do cliente da sua conexão do Site-to-Site VPN usando o console da Amazon VPC ou uma ferramenta de linha de comando.

Depois de alterar o gateway do cliente, a conexão VPN ficará indisponível durante um breve período enquanto provisionamos os novos endpoints.

Como alterar o gateway do cliente usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão VPN.
4. Escolha Ações, Modificar conexão VPN.
5. Em Tipo de destino, escolha Gateway do cliente.
6. Em Gateway do cliente de destino, escolha o novo gateway do cliente.
7. Escolha Salvar alterações.

Como excluir um gateway do cliente usando a linha de comando ou a API

- [ModifyVpnConnection](#) (API de consulta do Amazon EC2)
- [modify-vpn-connection](#) (AWS CLI)

Substituir as credenciais comprometidas para a conexão do Site-to-Site VPN

Caso suspeite que as credenciais do túnel para sua conexão do Site-to-Site VPN tenham sido comprometidas, altere a chave pré-compartilhada IKE ou altere o certificado do ACM. O método usado depende da opção de autenticação usada para seus túneis de VPN. Para ter mais informações, consulte [Opções de autenticação de túnel site a site VPN](#).

Alterar a chave pré-compartilhada IKE

É possível modificar as opções de túnel para a conexão VPN e especificar uma nova chave IKE pré-compartilhada para cada túnel. Para ter mais informações, consulte [Modificar opções de túnel do Site-to-Site VPN](#).

Como alternativa, é possível excluir a conexão VPN. Para ter mais informações, consulte [Excluir uma conexão VPN](#). Não é preciso excluir a VPC nem o gateway privado virtual. Depois, crie uma conexão VPN usando o mesmo gateway privado virtual e configure as novas chaves no dispositivo do gateway do cliente. Você pode especificar suas próprias chaves pré-compartilhadas para os túneis ou deixar AWS gerar novas chaves pré-compartilhadas para você. Para obter mais informações, consulte [Criar uma conexão VPN](#). Os endereços internos e externos do túnel podem mudar quando se cria novamente a conexão VPN.

Para alterar o certificado para o AWS lado do ponto final do túnel

Altere o certificado. Para ter mais informações, consulte [Alternar os certificados de endpoint do túnel da VPN](#).

Como alterar o certificado no dispositivo de gateway do cliente

1. Crie um novo certificado. Para obter informações, consulte [Emissão e gerenciamento de certificados](#) no Guia do usuário do AWS Certificate Manager .
2. Adicione o certificado ao dispositivo de gateway do cliente.

Alternar os certificados de endpoint do túnel do Site-to-Site VPN

Você pode alternar os certificados nos endpoints do túnel na AWS lateral usando o console da Amazon VPC. Quando o certificado de um endpoint de túnel está prestes a expirar, gira AWS automaticamente o certificado usando a função vinculada ao serviço. Para ter mais informações, consulte [the section called “Funções vinculadas a serviço”](#).

Como alternar o certificado de endpoint do túnel do Site-to-Site VPN usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Selecione a conexão do Site-to-Site VPN e escolha Ações, Modificar certificado de túnel VPN.
4. Selecione o endpoint do túnel.
5. Escolha Salvar.

Para alternar o certificado de ponto final do túnel VPN Site-to-Site usando o AWS CLI

Use o comando [modify-vpn-tunnel-certificate](#).

VPN IP privada com AWS Direct Connect

Com a VPN IP privada, você pode implantar a VPN IPsec AWS Direct Connect, criptografando o tráfego entre sua rede local e AWS sem o uso de endereços IP públicos ou equipamentos VPN adicionais de terceiros.

Um dos principais casos de uso da VPN IP privada AWS Direct Connect é ajudar clientes dos setores financeiro, de saúde e federal a cumprir as metas regulatórias e de conformidade. A VPN IP privada AWS Direct Connect garante que o tráfego entre redes locais AWS e redes locais seja seguro e privado, permitindo que os clientes cumpram suas exigências regulatórias e de segurança.

Conteúdo

- [Benefícios da VPN de IP privado](#)
- [Como funciona a VPN de IP privado](#)
- [Pré-requisitos](#)
- [Criar o gateway do cliente](#)
- [Preparar o gateway de trânsito](#)
- [Crie o AWS Direct Connect gateway](#)
- [Criar a associação a um gateway de trânsito](#)
- [Criar a conexão VPN](#)

Benefícios da VPN de IP privado

- Gerenciamento e operações de rede simplificados: sem VPN IP privada, os clientes precisam implantar VPN e roteadores de terceiros para implementar VPNs privadas em redes. AWS Direct Connect Com o recurso da VPN de IP privado, os clientes não precisam implantar nem gerenciar sua própria infraestrutura de VPN. Isso resulta em operações de rede simplificadas e custos reduzidos.
- Postura de segurança aprimorada: anteriormente, os clientes precisavam usar uma interface AWS Direct Connect virtual pública (VIF) para criptografar o tráfego AWS Direct Connect, o que exigia endereços IP públicos para endpoints de VPN. O uso de IPs públicos aumenta a probabilidade de ataques externos (DOS), o que, por sua vez, obriga os clientes a implantar equipamentos de segurança adicionais para proteção de rede. Além disso, uma VIF pública abre o acesso entre todos os serviços AWS públicos e as redes locais do cliente, aumentando a gravidade do risco.

O recurso VPN IP privado permite a criptografia em VIFs em AWS Direct Connect trânsito (em vez de VIFs públicas), juntamente com a capacidade de configurar IPs privados. Isso fornece conectividade end-to-end privada, além da criptografia, melhorando a postura geral de segurança.

- Maior escala de rota: as conexões VPN IP privadas oferecem limites de rota mais altos (5.000 rotas de saída e 1.000 rotas de entrada) em comparação com as conexões AWS Direct Connect isoladas, que atualmente têm um limite de 200 rotas de saída e 100 rotas de entrada.

Como funciona a VPN de IP privado

A VPN Site-to-Site com IP privado funciona em AWS Direct Connect uma interface virtual de trânsito (VIF). Ela usa um gateway do AWS Direct Connect e um gateway de trânsito para interconectar suas redes on-premises com as VPCs da AWS. Uma conexão VPN IP privada tem pontos de terminação no gateway de trânsito na AWS lateral e no dispositivo de gateway do cliente no lado local. Você deve atribuir endereços IP privados às extremidades do gateway de trânsito e do dispositivo de gateway do cliente dos túneis IPsec. Você pode usar endereços IP privados dos intervalos de endereços IPv4 privados RFC1918 ou RFC6598.

Anexe uma conexão VPN de IP privado a um gateway de trânsito. Depois, roteie o tráfego entre o anexo da VPN e qualquer VPC (ou outras redes) que também estejam anexadas ao gateway de trânsito. Isso é feito associando uma tabela de rotas ao anexo da VPN. Na direção inversa, você pode rotear o tráfego das VPCs para o anexo da VPN de IP privado usando tabelas de rotas associadas às VPCs.

A tabela de rotas associada ao anexo VPN pode ser a mesma ou diferente daquela associada ao AWS Direct Connect anexo subjacente. Isso oferece a possibilidade de rotear tráfego criptografado e não criptografado simultaneamente entre as VPCs e as redes on-premises.

Para obter mais detalhes sobre o caminho do tráfego que sai da VPN, consulte [Políticas de roteamento da interface virtual privada e da interface virtual de trânsito](#) no Guia do AWS Direct Connect usuário.

Pré-requisitos

Os seguintes recursos são necessários para concluir a configuração de uma VPN de IP privado sobre o AWS Direct Connect:

- Uma AWS Direct Connect conexão entre sua rede local e AWS
- Um AWS Direct Connect gateway com uma associação com o gateway de trânsito apropriado

- Um gateway de trânsito com um bloco CIDR de IP privado disponível
- Um dispositivo de gateway do cliente na rede on-premises e um gateway do cliente da AWS correspondente

Criar o gateway do cliente

Um gateway do cliente é um recurso que você cria em AWS. Ele representa o dispositivo de gateway do cliente na rede on-premises. Ao criar um gateway do cliente, você fornece informações sobre seu dispositivo para AWS. Para obter mais detalhes, consulte [Gateway do cliente](#).

Para criar um gateway do cliente usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Gateways do cliente.
3. Escolha Criar gateway do cliente.
4. (Opcional) Em Name (Nome), insira um nome para o gateway do cliente. Ao fazer isso, é criada uma tag com a chave Name e o valor especificado.
5. Para BGP ASN, informe o Número de sistema autônomo (ASN) do Border Gateway Protocol (BGP) do gateway do cliente.
6. Em IP address (Endereço IP), insira o endereço IP privado do dispositivo de gateway do cliente.
7. (Opcional) Para Device (Dispositivo), insira um nome para o dispositivo que hospeda esse gateway do cliente.
8. Escolha Criar gateway do cliente.

Para criar um gateway do cliente usando a linha de comando ou a API

- [CreateCustomerGateway](#) (API de consulta do Amazon EC2)
- [create-customer-gateway](#) (AWS CLI)

Preparar o gateway de trânsito

Um gateway de trânsito é um hub de trânsito de rede que pode ser usado para interconectar as VPCs e as redes on-premises. Você pode criar um gateway de trânsito ou usar um existente para a conexão da VPN de IP privado. Ao criar o gateway de trânsito ou modificar um existente, especifique um bloco CIDR de IP privado para a conexão.

Note

Ao especificar o bloco CIDR do gateway de trânsito a ser associado à VPN de IP privado, garanta que o bloco CIDR não se sobreponha a nenhum endereço IP referente a qualquer outro anexo de rede no gateway de trânsito. Se algum bloco CIDR IP se sobrepuer, isso poderá causar problemas de configuração com o dispositivo gateway do cliente.

Para ver as etapas específicas AWS do console para criar ou modificar um gateway de trânsito para usar na VPN IP privada, consulte [Transit Gateways](#) no Amazon VPC Transit Gateways Guide.

Para criar um gateway de trânsito usando a linha de comando ou a API

- [CreateTransitGateway](#)(API de consulta do Amazon EC2)
- [create-transit-gateway](#) (AWS CLI)

Crie o AWS Direct Connect gateway

Crie um AWS Direct Connect gateway seguindo o procedimento [Criando um gateway Direct Connect](#) no Guia AWS Direct Connect do usuário.

Para criar um AWS Direct Connect gateway usando a linha de comando ou a API

- [CreateDirectConnectGateway](#)(API AWS Direct Connect de consulta)
- [create-direct-connect-gateway](#) (AWS CLI)

Criar a associação a um gateway de trânsito

Depois de criar o AWS Direct Connect gateway, crie uma associação de gateway de trânsito para o AWS Direct Connect gateway. Especifique o CIDR de IP privado para o gateway de trânsito identificado anteriormente na lista de prefixos permitidos.

Para obter mais informações, consulte [Associações do gateway de trânsito](#) no Guia do usuário do AWS Direct Connect .

Para criar uma associação de AWS Direct Connect gateway usando a linha de comando ou a API

- [CreateDirectConnectGatewayAssociation](#)(API AWS Direct Connect de consulta)

- [create-direct-connect-gateway-associação](#) ()AWS CLI

Criar a conexão VPN

Como criar uma conexão VPN usando endereços IP privados

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões VPN de local a local.
3. Escolha Create VPN Connection (Criar conexão VPN).
4. (Opcional) Em Name tag (Marcação de nome), insira um nome para a conexão de VPN de local a local. Ao fazer isso, é criada uma marcação com a chave de Name e o valor que você especificar.
5. Em Target gateway type (Tipo de gateway de destino), escolha Transit gateway (Gateway de trânsito). Depois, selecione o gateway de trânsito identificado anteriormente.
6. Em Customer gateway (Gateway do cliente), selecione Existing (Existente). Depois, selecione o gateway do cliente criado anteriormente.
7. Escolha uma das opções de roteamento dependendo se o seu dispositivo de gateway do cliente oferece suporte ao Border Gateway Protocol (BGP):
 - Se o dispositivo de gateway do cliente oferecer suporte ao BGP, selecione Dynamic (requires BGP) (Dinâmico [requer BGP]).
 - Se o dispositivo de gateway do cliente não oferecer suporte ao BGP, selecione Static (Estático).
8. Em Versão IP de túnel interno, especifique se os túneis VPN são compatíveis com tráfego IPv4 ou IPv6.
9. (Opcional) Se você especificou IPv4 para túnel dentro da versão IP, você pode, opcionalmente, especificar os intervalos de CIDR IPv4 para o gateway do cliente e AWS os lados que têm permissão para se comunicar pelos túneis VPN. O padrão é 0.0.0.0/0.

Se você especificou IPv6 para túnel dentro da versão IP, você pode, opcionalmente, especificar os intervalos de CIDR IPv6 para o gateway do cliente e AWS os lados que têm permissão para se comunicar pelos túneis VPN. O padrão para ambos os intervalos é ::/0.
10. Em Tipo de endereço IP externo, escolha PrivateIpv4.
11. Em ID do anexo de transporte, escolha o anexo do gateway de trânsito para o AWS Direct Connect gateway apropriado.

12. Escolha Create VPN Connection (Criar conexão VPN).

Note

A opção Enable acceleration (Habilitar a aceleração) não é aplicável para conexões VPN sobre o AWS Direct Connect.

Segurança em AWS site a site VPN

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isso como segurança da nuvem e segurança na nuvem:

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas AWS de conformidade que se aplicam ao site a siteVPN, consulte [AWS Serviços no escopo do programa de conformidade AWS Serviços no escopo do programa](#) conformidade.
- **Segurança na nuvem** — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar Site-to-SiteVPN. Os tópicos a seguir mostram como configurar site a site para atender VPN aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos de site a site. VPN

Conteúdo

- [Proteção de dados em AWS site a site VPN](#)
- [Gerenciamento de identidade e acesso para AWS site a site VPN](#)
- [Resiliência em AWS Site-to-Site VPN](#)
- [Segurança da infraestrutura em AWS site a site VPN](#)

Proteção de dados em AWS site a site VPN

O [modelo de responsabilidade AWS compartilhada](#) se aplica à proteção de dados em AWS site a siteVPN. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo

hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte [Privacidade de dados FAQ](#). Para obter informações sobre proteção de dados na Europa, consulte o [Modelo de Responsabilidade AWS Compartilhada e GDPR](#) a postagem no blog AWS de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use a autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou uma API, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-3](#).

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com Site-to-Site VPN ou outro Serviços da AWS usando o console, API, AWS CLI ou AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Privacidade do tráfego entre redes

Uma VPN conexão site a site conecta você de forma privada VPC à sua rede local. Os dados transferidos entre você VPC e sua rede são roteados por meio de uma VPN conexão criptografada para ajudar a manter a confidencialidade e a integridade dos dados em trânsito. A Amazon oferece suporte a VPN conexões de segurança do Internet Protocol (IPsec). IPsec é um conjunto de protocolos para proteger as comunicações IP autenticando e criptografando cada pacote IP em um fluxo de dados.

Cada VPN conexão site a site consiste em dois IPsec VPN túneis criptografados que se conectam à sua rede. AWS O tráfego em cada túnel pode ser criptografado com AES128 ou AES256 e usar grupos Diffie-Hellman para troca de chaves, fornecendo Perfect Forward Secrecy. AWS autentica com funções de hashing SHA1 ou de SHA2 hashing.

As suas instâncias VPC não exigem um endereço IP público para se conectar aos recursos do outro lado da sua conexão de site a site. VPN As instâncias podem rotear o tráfego da Internet por meio da VPN conexão site a site com sua rede local. Elas podem acessar a Internet por meio de seus pontos de tráfego de saída existentes e seus dispositivos de segurança e monitoramento de rede.

Consulte os tópicos a seguir para obter mais informações:

- [Opções de túnel para a conexão do Site-to-Site VPN](#): fornece informações sobre as opções IPsec e o Internet Key Exchange (IKE) que estão disponíveis para cada túnel.
- [Opções de autenticação de túnel site a site VPN](#): fornece informações sobre as opções de autenticação para seus endpoints de VPN túnel.
- [Requisitos do seu dispositivo de gateway do cliente](#): fornece informações sobre os requisitos do dispositivo de gateway do cliente no seu lado da VPN conexão.
- [Fornecendo comunicação segura entre sites usando VPN CloudHub](#): Se você tiver várias VPN conexões de site a site, poderá fornecer comunicação segura entre seus sites locais usando o AWS VPN CloudHub

Gerenciamento de identidade e acesso para AWS site a site VPN

AWS Identity and Access Management (IAM) é uma ferramenta Serviço da AWS que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. IAM os administradores

controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar recursos de site a siteVPN. IAM é um Serviço da AWS que você pode usar sem custo adicional.

Tópicos

- [Público](#)
- [Autenticando com identidades](#)
- [Gerenciando acesso usando políticas](#)
- [Como funciona AWS o site a site com VPN IAM](#)
- [Exemplos de políticas baseadas em identidade para site a site AWS VPN](#)
- [Solução de problemas de AWS identidade e acesso de site a site VPN](#)
- [Usando funções vinculadas a serviços para site a site VPN](#)

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz em Site-to-SiteVPN.

Usuário do serviço — Se você usar o VPN serviço Site-to-Site para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais VPN recursos de site a site para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no Site-to-SiteVPN, consulte. [Solução de problemas de AWS identidade e acesso de site a site VPN](#)

Administrador de serviços — Se você é responsável pelos recursos de site a site em sua empresa, provavelmente tem acesso total aos VPN recursos de site a site. VPN É seu trabalho determinar quais VPN recursos e recursos de site a site seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos do IAM. Para saber mais sobre como sua empresa pode usar o IAM Site-to-SiteVPN, consulte. [Como funciona AWS o site a site com VPN IAM](#)

IAM administrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao site a site. VPN Para ver exemplos de políticas VPN baseadas em identidade de site a site que você pode usar em, consulte. IAM [Exemplos de políticas baseadas em identidade para site a site AWS VPN](#)

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como IAM usuário ou assumindo uma IAM função. Usuário raiz da conta da AWS

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte [Como fazer login Conta da AWS no](#) Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para você mesmo assinar solicitações, consulte [Assinar AWS API solicitações](#) no Guia IAM do usuário.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte [Autenticação multifator](#) no Guia AWS IAM Identity Center do usuário e [Uso da autenticação multifator \(MFA\) AWS no](#) Guia do IAM usuário.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte [Tarefas que exigem credenciais de usuário raiz](#) no Guia do IAM usuário.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter informações sobre o IAM Identity Center, consulte [O que é o IAM Identity Center?](#) no Guia do AWS IAM Identity Center usuário.

Grupos e usuários do IAM

Um [IAMusuário](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários que tenham credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte [Altere as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo](#) no Guia do IAMusuário.

Um [IAMgrupo](#) é uma identidade que especifica uma coleção de IAM usuários. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Quando criar um IAM usuário \(em vez de uma função\)](#) no Guia do IAM usuário.

IAMfunções

Uma [IAMfunção](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console [trocando de funções](#). Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte [Usando IAM funções](#) no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte [Criação de uma função para um provedor de identidade terceirizado](#) no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no Manual do Usuário do AWS IAM Identity Center .
- **Permissões temporárias IAM de IAM usuário** — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- **Acesso entre contas** — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte [Acesso a recursos entre contas IAM no Guia](#) do IAM usuário.
- **Acesso entre serviços** — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
 - **Sessões de acesso direto (FAS)** — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FAS usa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para

fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte [Encaminhar sessões de acesso](#).

- Função de serviço — Uma função de serviço é uma [IAMfunção](#) que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte [Criação de uma função para delegar permissões a uma Serviço da AWS](#) no Guia do IAM usuário.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. Serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte [Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon](#) no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte [Quando criar uma IAM função \(em vez de um usuário\)](#) no Guia do IAM usuário.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte [Visão geral das JSON políticas](#) no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criação de IAM políticas no Guia](#) do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte [Escolha entre políticas gerenciadas e políticas em linha no Guia](#) do IAMusuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a [visão geral da lista de controle de acesso \(ACL\)](#) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- **Limites de permissões** — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAM usuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para IAM entidades](#) no Guia IAM do usuário.
- **Políticas de controle de serviço (SCPs)** — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte [Políticas de controle de serviços](#) no Guia AWS Organizations do Usuário.
- **Políticas de sessão:** são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do

usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia IAM do usuário.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de política estão envolvidos, consulte [Lógica de avaliação](#) de políticas no Guia IAM do usuário.

Como funciona AWS o site a site com VPN IAM

Antes de usar IAM para gerenciar o acesso ao Site-to-SiteVPN, saiba quais IAM recursos estão disponíveis para uso com o Site-to-Site. VPN

IAMrecursos que você pode usar com AWS Site-to-Site VPN

IAMrecurso	Suporte site a site VPN
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC(tags nas políticas)	Não
Credenciais temporárias	Sim
Permissões de entidade principal	Sim

IAMrecurso	Suporte site a site VPN
Perfis de serviço	Sim
Funções vinculadas a serviço	Sim

Para obter uma visão geral de como o Site-to-Site VPN e outros AWS serviços funcionam com a maioria dos IAM recursos, consulte [AWS os serviços que funcionam com IAM](#) no Guia do Usuário. IAM

Políticas baseadas em identidade para site a site VPN

Compatível com políticas baseadas em identidade: Sim

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criação de IAM políticas no Guia](#) do IAMusuário.

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a [referência IAM JSON de elementos de política](#) no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para site a site VPN

Para ver exemplos de políticas baseadas em VPN identidade de site a site, consulte. [Exemplos de políticas baseadas em identidade para site a site AWS VPN](#)

Políticas baseadas em recursos dentro de site a site VPN

Suporte a políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os

administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para habilitar o acesso entre contas, você pode especificar uma conta ou IAM entidades inteiras em outra conta como principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um IAM administrador na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, [consulte Acesso a recursos entre contas IAM no](#) Guia do IAM usuário.

Ações políticas para site a site VPN

Compatível com ações de políticas: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente com permissão que não têm uma operação correspondente. API Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações de site a site, consulte VPN [Ações definidas por site a AWS site na Referência de autorização de serviço VPN](#).

As ações de política em Site-to-Site VPN usam o seguinte prefixo antes da ação:

```
ec2
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [  
  "ec2:action1",  
  "ec2:action2"  
]
```

Para ver exemplos de políticas baseadas em VPN identidade de site a site, consulte [Exemplos de políticas baseadas em identidade para site a site AWS VPN](#)

Recursos de política para site a site VPN

Compatível com recursos de políticas: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento Resource JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento Resource ou NotResource. Como prática recomendada, especifique um recurso usando seu [Amazon Resource Name \(ARN\)](#). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de VPN recursos de site a site e seus ARNs, consulte [Recursos definidos por site a AWS site na Referência de autorização de serviço VPN](#). Para saber com quais ações você pode especificar cada recurso, consulte [Ações definidas por AWS site a site. ARN VPN](#)

Para ver exemplos de políticas baseadas em VPN identidade de site a site, consulte [Exemplos de políticas baseadas em identidade para site a site AWS VPN](#)

Chaves de condição de política para site a site VPN

Compatível com chaves de condição de política específicas de serviço: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem [agentes de condição](#), como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica AND. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma OR operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte [elementos de IAM política: variáveis e tags](#) no Guia IAM do usuário.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia IAM do usuário.

Para ver uma lista de chaves de VPN condição de site a site, consulte Chaves de [condição de site a AWS site na Referência de autorização de serviço VPN](#). Para saber com quais ações e recursos você pode usar uma chave [AWS de condição, consulte Ações definidas por site a site VPN](#).

Para ver exemplos de políticas baseadas em VPN identidade de site a site, consulte. [Exemplos de políticas baseadas em identidade para site a site AWS VPN](#)

ACLsem Site-to-Site VPN

SuportesACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

ABACcom Site-to-Site VPN

Suportes ABAC (tags nas políticas): Não

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a IAM entidades (usuários ou funções) e a muitos AWS recursos. Marcar entidades e recursos é a primeira etapa do ABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna complicado.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no [elemento de condição](#) de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre ABAC, consulte [O que é ABAC?](#) no Guia do IAM usuário. Para ver um tutorial com etapas de configuração ABAC, consulte [Usar controle de acesso baseado em atributos \(ABAC\) no Guia](#) do IAM usuário.

Usando credenciais temporárias com Site-to-Site VPN

Compatível com credenciais temporárias: Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte [Serviços da AWS nesse trabalho IAM](#) no Guia do IAM usuário.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre a troca de funções, consulte [Alternando para uma função \(console\)](#) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte [Credenciais de segurança temporárias em IAM](#).

Permissões principais entre serviços para site a site VPN

Suporta sessões de acesso direto (FAS): Sim

Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FAS usa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para fazer solicitações aos serviços posteriores. FAS as solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte [Encaminhar sessões de acesso](#).

Funções de serviço para site a site VPN

Compatível com perfis de serviço: Sim

Uma função de serviço é uma [IAM função](#) que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamente IAM. Para obter mais informações, consulte [Criação de uma função para delegar permissões a uma Serviço da AWS](#) no Guia do IAM usuário.

Warning

Alterar as permissões de uma função de serviço pode interromper a funcionalidade de site a site VPN. Edite as funções de serviço somente quando o site a site VPN fornecer orientação para fazer isso.

Funções vinculadas a serviços para site a site VPN

Suporte a perfis vinculados a serviços: sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um Serviço da AWS. O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte [AWS serviços que funcionam](#) com IAM. Encontre um serviço na tabela que inclua um Yes na coluna

Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para site a site AWS VPN

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos de site a site. VPN Eles também não podem realizar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos de JSON política, consulte [Criação de IAM políticas no Guia](#) do IAM usuário.

Para obter detalhes sobre ações e tipos de recursos definidos por Site-to-SiteVPN, incluindo o formato de cada um dos ARNs tipos de recursos, consulte [Ações, recursos e chaves de condição para AWS Site-to-Site VPN](#) na Referência de Autorização de Serviço.

Tópicos

- [Melhores práticas de política](#)
- [Usando o console Site-to-Site VPN](#)
- [Descrever conexões específicas de site a site VPN](#)
- [Crie e descreva os recursos necessários para uma AWS Site-to-Site VPN conexão](#)

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos de site a site em sua contaVPN. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte [políticas AWS gerenciadas](#) ou [políticas AWS gerenciadas para funções de trabalho](#) no Guia IAM do usuário.

- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte [Políticas e permissões IAM no Guia IAM do usuário](#).
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica Serviço da AWS, como AWS CloudFormation. Para obter mais informações, consulte [elementos IAM JSON da política: Condição](#) no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação da política do IAM Access Analyzer](#) no Guia do IAM Usuário.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte [Configurando o API acesso MFA protegido](#) no Guia do IAM usuário.

Para obter mais informações sobre as melhores práticas em IAM, consulte [as melhores práticas de segurança IAM no Guia IAM do usuário](#).

Usando o console Site-to-Site VPN

Para acessar o VPN console AWS Site-to-Site, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os VPN recursos de site a site em seu. Conta da AWS Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para AWS CLI o. ou AWS API o. Em vez disso, permita o acesso somente às ações que correspondam à API operação que eles estão tentando realizar.

Para garantir que usuários e funções ainda possam usar o VPN console Site-to-Site, anexe também a política Site-to-Site VPN AmazonVPCFullAccess ou AmazonVPCReadOnlyAccess AWS gerenciada às entidades. Para obter mais informações, consulte [Adicionar permissões a um usuário](#) no Guia do IAM usuário.

Descrever conexões específicas de site a site VPN

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpnConnections"
      ],
      "Resource": [
        "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-04d5cc9b88example",
        "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-903004f88example"
      ]
    }
  ]
}
```

Crie e descreva os recursos necessários para uma AWS Site-to-Site VPN conexão

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:DescribeCustomerGateways",
        "ec2:CreateCustomerGateway",
        "ec2:CreateVpnGateway",
        "ec2:CreateVpnConnection"
      ],
      "Resource": [
        "*"
      ]
    }
  ],
}
```

```
{
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "arn:aws:iam::*:role/aws-service-role/s2svpn.amazonaws.com/
AWSServiceRoleForVPCS2SVPNInternal",
  "Condition": {
    "StringLike": {
      "iam:AWSServiceName": "s2svpn.amazonaws.com"
    }
  }
}
```

Solução de problemas de AWS identidade e acesso de site a site VPN

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com Site-to-Site e VPN IAM

Tópicos

- [Não estou autorizado a realizar uma ação em Site-to-Site VPN](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora do meu acessem meus recursos de site Conta da AWS VPN a site](#)

Não estou autorizado a realizar uma ação em Site-to-Site VPN

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

O exemplo de erro a seguir ocorre quando o mateojackson IAM usuário tenta usar o console para ver detalhes sobre um *my-example-widget* recurso fictício, mas não tem as permissões fictíciasec2:*GetWidget*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
ec2:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso `my-example-widget` usando a ação `ec2:GetWidget`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar `iam:PassRole`

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para site a siteVPN.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um IAM usuário chamado `marymajor` tenta usar o console para realizar uma ação em Site a SiteVPN. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora do meu acessem meus recursos de site Conta da AWS VPN a site

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o site a site VPN oferece suporte a esses recursos, consulte. [Como funciona AWS o site a site com VPN IAM](#)

- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte [Fornecer acesso a um IAM usuário em outro Conta da AWS de sua propriedade](#) no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte [Fornecer Contas da AWS acesso a terceiros](#) no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte [Fornecendo acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do IAM usuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a [recursos entre contas IAM no Guia](#) do IAM usuário.

Usando funções vinculadas a serviços para site a site VPN

AWS [Site a site VPN usa AWS Identity and Access Management \(IAM\) funções vinculadas ao serviço](#). Uma função vinculada ao serviço é um tipo exclusivo de IAM função vinculada diretamente ao site a site. VPN As funções vinculadas ao serviço são predefinidas pelo site a site VPN e incluem todas as permissões que o serviço exige para chamar outros serviços em seu nome. AWS

Uma função vinculada ao serviço facilita a configuração de site a site VPN porque você não precisa adicionar manualmente as permissões necessárias. Site a site VPN define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente site a site VPN pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra IAM entidade.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege seus VPN recursos de site a site porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte [AWS Serviços que funcionam com IAM](#) e procure os serviços que têm Sim na coluna Funções vinculadas ao serviço. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculadas ao serviço para site a site VPN

Site a site VPN usa a função vinculada ao serviço chamada `AWSServiceRoleForVPCS2SVPN`— Permitir que site a site crie e gerencie recursos relacionados VPN às suas conexões. VPN

A função `AWSServiceRoleForVPCS2SVpn` vinculada ao serviço confia nos seguintes serviços para assumir a função:

- AWS Certificate Manager
- AWS Private Certificate Authority

A política de permissões de função denominada `AWSVPCS2SVpnServiceRolePolicy` permite que Site-to-Site VPN conclua as seguintes ações nos recursos especificados:

- Ação: `acm:ExportCertificate` em Resource: `"*"`
- Ação: `acm:DescribeCertificate` em Resource: `"*"`
- Ação: `acm:ListCertificates` em Resource: `"*"`
- Ação: `acm-pca:DescribeCertificateAuthority` em Resource: `"*"`

Você deve configurar permissões para permitir que uma IAM entidade (como usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte [Permissões de funções vinculadas ao serviço](#) no Guia do IAM usuário.

Criação de uma função vinculada ao serviço para site a site VPN

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria um gateway do cliente com um certificado ACM privado associado no AWS Management Console, no ou no AWS CLI AWS API, Site-to-Site VPN cria a função vinculada ao serviço para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você cria um gateway do cliente com um certificado ACM privado associado, o Site-to-Site VPN cria a função vinculada ao serviço para você novamente.

Editando uma função vinculada ao serviço para site a site VPN

O site a site VPN não permite que você edite a função vinculada ao `AWSServiceRoleForVPCS2SVpn` serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, você pode editar a descrição da função usando IAM. Para obter mais informações, consulte [Edição de uma função vinculada ao serviço](#) no Guia do IAM usuário.

Excluindo uma função vinculada ao serviço para site a site VPN

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

Note

Se o VPN serviço Site-to-Site estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir VPN recursos de site a site usados pelo `AWSServiceRoleForVPCS2SVPN`

Você pode excluir essa função vinculada ao serviço somente depois de excluir todos os gateways do cliente que tenham um certificado privado associado ACM. Isso garante que você não possa remover inadvertidamente a permissão para acessar seus ACM certificados em uso por conexões site a site. VPN

Para excluir manualmente a função vinculada ao serviço usando IAM

Use o IAM console AWS CLI, o ou o AWS API para excluir a função `AWSServiceRoleForVPCS2SVPN` vinculada ao serviço. Para obter mais informações, consulte [Excluindo uma função vinculada ao serviço no Guia](#) do IAM usuário.

Resiliência em AWS Site-to-Site VPN

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

Além da infraestrutura AWS global, o Site-to-Site VPN oferece recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Dois túneis por conexão VPN

Uma VPN conexão site a site consiste em dois túneis, cada um terminando em uma zona de disponibilidade diferente, para fornecer maior disponibilidade para você. VPC Se houver uma falha no dispositivo AWS, sua VPN conexão automaticamente passará para o segundo túnel para que seu acesso não seja interrompido. De tempos em tempos, AWS também realiza manutenção de rotina em sua VPN conexão, o que pode desativar brevemente um dos dois túneis de sua VPN conexão. Para obter mais informações, consulte [Substituições de endpoint de túnel Site-to-Site VPN](#). Ao configurar o gateway do cliente, é importante configurar ambos os túneis.

Redundância

Para se proteger contra a perda de conectividade caso o gateway do cliente fique indisponível, você pode configurar uma segunda conexão site a siteVPN. Para obter mais informações, consulte a seguinte documentação do :

- [Utilização de conexões do Site-to-Site VPN redundantes para realizar failover](#)
- [Opções de conectividade da Amazon Virtual Private Cloud](#)
- [Construindo uma infraestrutura de rede múltipla escalável e segura VPC AWS](#)

Segurança da infraestrutura em AWS site a site VPN

Como um serviço gerenciado, o AWS Site-to-Site VPN é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte [AWS Cloud Security](#). Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte [Proteção](#) de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa API chamadas AWS publicadas para acessar site a site VPN pela rede. Os clientes devem oferecer suporte para:

- Segurança da camada de transporte (TLS). Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Suítes de criptografia com sigilo direto perfeito (), como (Ephemeral PFS Diffie-Hellman) ou DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Monitorar a conexão do Site-to-Site VPN

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho da sua AWS Site-to-Site VPN conexão. Você deve coletar dados de monitoramento de todas as partes de sua solução para facilitar a depuração de uma falha multipontos, caso ocorra. Antes de começar a monitorar sua conexão do Site-to-Site VPN, você deve criar um plano de monitoramento que inclui respostas às seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

A próxima etapa é estabelecer um parâmetro de performance normal da VPN no ambiente medindo a performance em vários momentos e em diferentes condições de carga. À medida que você monitorar a VPN, armazene dados históricos de monitoramento para que possa compará-los com os dados de performance atuais, identificar padrões de performance normais e anomalias de performance e idealizar métodos para solucionar problemas.

Para estabelecer um parâmetro, é preciso monitorar os seguintes itens:

- O estado dos túneis da VPN
- Os dados no túnel
- Os dados fora do túnel

Tópicos

- [Ferramentas de monitoramento](#)
- [AWS Site-to-Site VPN troncos](#)
- [Monitoramento de túneis VPN usando a Amazon CloudWatch](#)
- [Monitoramento de conexões VPN usando AWS Health eventos](#)

Ferramentas de monitoramento

AWS fornece várias ferramentas que você pode usar para monitorar uma conexão VPN Site-to-Site. É possível configurar algumas dessas ferramentas para fazer o monitoramento em seu lugar, e, ao mesmo tempo, algumas das ferramentas exigem intervenção manual. Recomendamos que as tarefas de monitoramento sejam automatizadas ao máximo possível.

Ferramentas de monitoramento automatizadas

Você pode usar as seguintes ferramentas de monitoramento automatizadas para observar uma conexão do Site-to-Site VPN e relatar um erro quando necessário:

- Amazon CloudWatch Alarms — Observe uma única métrica em um período especificado por você e execute uma ou mais ações com base no valor da métrica em relação a um determinado limite em vários períodos. A ação é uma notificação enviada para um tópico do Amazon SNS. CloudWatch os alarmes não invocam ações simplesmente porque estão em um determinado estado; o estado deve ter sido alterado e mantido por um determinado número de períodos. Para ter mais informações, consulte [Monitoramento de túneis VPN usando a Amazon CloudWatch](#).
- AWS CloudTrail Monitoramento de registros — compartilhe arquivos de log entre contas, monitore arquivos de CloudTrail log em tempo real enviando-os para o CloudWatch Logs, grave aplicativos de processamento de log em Java e valide se seus arquivos de log não foram alterados após a entrega. CloudTrail Para obter mais informações, consulte [Registro de chamadas de API usando AWS CloudTrail](#) na Referência de API do Amazon EC2 e [Trabalho com arquivos de CloudTrail log](#) no Guia do AWS CloudTrail usuário.
- AWS Health eventos — receba alertas e notificações relacionados a alterações na integridade de seus túneis VPN Site-to-Site, recomendações de configuração de melhores práticas ou ao se aproximar dos limites de escalabilidade. Use eventos no [Personal Health Dashboard](#) para acionar failovers automatizados, reduzir o tempo de solução de problemas ou otimizar conexões para alta disponibilidade. Para obter mais informações, consulte [Monitoramento de conexões VPN usando AWS Health eventos](#).

Ferramentas de monitoramento manual

Outra parte importante do monitoramento de uma conexão VPN Site-to-Site envolve o monitoramento manual dos itens que CloudWatch os alarmes não cobrem. Os painéis do Amazon VPC e CloudWatch do console fornecem uma at-a-glance visão do estado do seu ambiente. AWS

Note

No console da Amazon VPC, os parâmetros de estado do túnel VPN Site-to-Site, como “Status” e “Última alteração de status”, podem não refletir mudanças de estado transitórias ou oscilações momentâneas do túnel. É recomendável usar CloudWatch métricas e registros para atualizações granulares de alterações de estado do túnel.

- O painel da Amazon VPC mostra:
 - Integridade do serviço por região
 - Conexões Site-to-Site VPN
 - Status do túnel VPN (no painel de navegação, escolha Site-to-Site VPN Connections (Conexões do Site-to-Site VPN), selecione uma conexão do Site-to-Site VPN e escolha Tunnel Details (Detalhes do túnel))
- A página CloudWatch inicial mostra:
 - Alertas e status atual
 - Gráficos de alertas e recursos
 - Estado de integridade do serviço

Além disso, você pode usar CloudWatch para fazer o seguinte:

- Crie [painéis personalizados](#) para monitorar os serviços com os quais você se preocupa.
- Colocar em gráfico dados de métrica para solucionar problemas e descobrir tendências
- Pesquise e navegue em todas as suas métricas AWS de recursos
- Criar e editar alertas para ser notificado sobre problemas

AWS Site-to-Site VPN troncos

AWS Site-to-Site VPN os registros fornecem uma visibilidade mais profunda de suas implantações de VPN Site-to-Site. Com esse recurso, você pode ter acesso a logs de conexão do Site-to-Site VPN que fornecem detalhes sobre estabelecimento do túnel de segurança IP (IPsec), negociações do Internet Key Exchange (IKE) e mensagens de protocolo Dead Peer Detection (DPD).

Os registros de VPN site-to-site podem ser publicados no Amazon Logs. CloudWatch Esse recurso fornece aos clientes uma maneira única e consistente de acessar e analisar logs detalhados de todas as conexões do Site-to-Site VPN.

Conteúdo

- [Benefícios dos logs do Site-to-Site VPN](#)
- [Restrições de tamanho da política de recursos do Amazon CloudWatch Logs](#)
- [Conteúdo dos logs do Site-to-Site VPN](#)
- [Requisitos do IAM para publicar no CloudWatch Logs](#)
- [Exibir configuração de logs do Site-to-Site VPN](#)
- [Habilitar os logs do Site-to-Site VPN](#)
- [Desabilitar logs do Site-to-Site VPN](#)

Benefícios dos logs do Site-to-Site VPN

- Solução de problemas simplificada de VPN: os registros de VPN site-to-site ajudam você a identificar incompatibilidades de configuração AWS entre o dispositivo de gateway do cliente e a resolver os problemas iniciais de conectividade da VPN. As conexões VPN podem oscilar intermitentemente ao longo do tempo devido a configurações incorretas (como tempos limite mal ajustados). Pode haver problemas nas redes de transporte subjacentes (como clima da Internet) ou alterações de roteamento ou falhas de caminho podem provocar interrupção da conectividade pela VPN. Esse recurso permite diagnosticar com precisão a causa de falhas de conexão intermitentes e ajustar a configuração do túnel de baixo nível para uma operação confiável.
- AWS Site-to-Site VPN Visibilidade centralizada: os registros de VPN site a site podem fornecer registros de atividades de túneis para todas as diferentes maneiras pelas quais a VPN site a site está conectada: gateway virtual, gateway de trânsito e, usando a Internet e como transporte. CloudHub AWS Direct Connect Esse recurso fornece aos clientes uma maneira única e consistente de acessar e analisar logs detalhados de todas as conexões do Site-to-Site VPN.
- Segurança e conformidade: os registros de VPN site-to-site podem ser enviados ao CloudWatch Amazon Logs para análise retrospectiva do status e da atividade da conexão VPN ao longo do tempo. Isso pode ajudar você a atender a requisitos de conformidade e regulamentares.

Restrições de tamanho da política de recursos do Amazon CloudWatch Logs

CloudWatch As políticas de recursos de registros estão limitadas a 5120 caracteres. Quando o CloudWatch Logs detecta que uma política se aproxima desse limite de tamanho, ele ativa

automaticamente grupos de registros que começam com `/aws/vendedlogs/`. Quando você ativa o registro, a VPN Site-to-Site deve atualizar CloudWatch sua política de recursos de registros com o grupo de registros especificado. Para evitar atingir o limite de tamanho da política de recursos de CloudWatch registros, prefixe os nomes dos grupos de registros com `/aws/vendedlogs/`.

Conteúdo dos logs do Site-to-Site VPN

As informações a seguir estão incluídas no log de atividades do túnel do Site-to-Site VPN.

Campo	Descrição
VpnLogCreationTimestamp	Carimbo de data/hora de criação do log em formato legível por humanos.
VpnConnectionId	O identificador da conexão VPN.
TunnelOutsideEndereço IP	O IP externo do túnel VPN que gerou a entrada de log.
TunnelDPDEnabled	Status habilitado do protocolo Dead Peer Detection (True/False).
Túnel CGW Natt DetectionStatus	NAT-T detectado no dispositivo de gateway do cliente (True/False).
TunnelIKEPhase1State	Estado do protocolo IKE Fase 1 (Established Rekeying Negotiating Down).
TunnelIKEPhase2State	Estado do protocolo IKE Fase 2 (Established Rekeying Negotiating Down).
VpnLogDetail	Mensagens detalhadas para protocolos IPsec, IKE e DPD.

Conteúdo

- [Mensagens de erro do IKEv1](#)
- [Mensagens de erro do IKEv2](#)
- [Mensagens de negociação do IKEv2](#)

Mensagens de erro do IKEv1

Message	Explicação
O par não responde: declaração de par desativado	O par não respondeu às mensagens de DPD, aplicando a ação de tempo limite de DPD.
AWS A decodificação da carga útil do túnel não teve êxito devido à chave pré-compartilhada inválida	A mesma chave pré-compartilhada precisa ser configurada em ambos os pares do IKE.
Nenhuma proposta correspondente encontrada por AWS	Os atributos propostos para a fase 1 (criptografia, hashing e grupo DH) não são compatíveis com o endpoint da AWS VPN. Por exemplo, 3DES
Nenhuma proposta correspondente encontrada. Notificação com "Nenhuma proposta escolhida"	Nenhuma mensagem de erro da proposta escolhida é trocada entre os pares para informar que as propostas/políticas corretas devem ser configuradas para a fase 2 em pares do IKE.
AWS o túnel recebeu DELETE para a fase 2 SA com SPI: xxxx	O CGW enviou a mensagem Delete_SA para a Fase 2
AWS túnel recebeu DELETE para IKE_SA da CGW	O CGW enviou a mensagem Delete_SA para a Fase 1

Mensagens de erro do IKEv2

Message	Explicação
AWS O tempo limite do DPD do túnel foi atingido após a retransmissão de {retry_count}	O par não respondeu às mensagens de DPD, aplicando a ação de tempo limite de DPD.
AWS túnel recebeu DELETE para IKE_SA da CGW	O par enviou a mensagem Delete_SA para Parent/IKE_SA

Message	Explicação
AWS o túnel recebeu DELETE para a fase 2 SA com SPI: xxxx	O par enviou a mensagem Delete_SA para CHILD_SA
AWS o túnel detectou uma colisão (CHILD_REKEY) como CHILD_DELETE	O CGW enviou a mensagem Delete_SA para o SA ativo, que está sendo recodificado.
AWS A SA redundante do túnel (CHILD_SA) está sendo excluída devido à colisão detectada	Devido à colisão, se SAs redundantes forem gerados, os pares fecharão o SA redundante e depois de combinar os valores de nonce de acordo com o RFC
AWS O túnel da Fase 2 não foi capaz de se estabelecer enquanto mantinha a Fase 1	O par não conseguiu estabelecer CHILD_SA devido a um erro de negociação; por exemplo, proposta incorreta.
AWS: seletor de tráfego: TS_UNACCEPTABLE: recebido do respondente	O par propôs seletores de tráfego/domínio de criptografia incorretos. Os pares devem ser configurados com CIDRs idênticos e corretos.
AWS o túnel está enviando AUTHENTICATION_FAILED como resposta	O par não consegue autenticar o par verificando o conteúdo da mensagem IKE_AUTH
AWS o túnel detectou uma incompatibilidade de chave pré-compartilhada com cgw: xxxx	A mesma chave pré-compartilhada precisa ser configurada em ambos os pares do IKE.
AWS Tempo limite do túnel: excluindo IKE_SA da Fase 1 não estabelecida com cgw: xxxx	A exclusão do IKE_SA semiaberto como par não prosseguiu com as negociações
Nenhuma proposta correspondente encontrada. Notificação com "Nenhuma proposta escolhida"	Nenhuma mensagem de erro da proposta escolhida é trocada entre os pares para informar que as propostas corretas devem ser configuradas em pares do IKE.
Nenhuma proposta correspondente encontrada por AWS	Os atributos propostos para a fase 1 (criptografia, hashing e grupo DH) não são suportados pelo AWS VPN Endpoint. Por exemplo, 3DES

Mensagens de negociação do IKEv2

Message	Explicação
AWS solicitação processada por túnel (id=xxx) para CREATE_CHILD_SA	AWS recebeu a solicitação CREATE_CHILD_SA da CGW
AWS o túnel está enviando resposta (id=xxx) para CREATE_CHILD_SA	AWS está enviando a resposta CREATE_CHILD_SA para o CGW
AWS o túnel está enviando a solicitação (id=xxx) para CREATE_CHILD_SA	AWS está enviando a solicitação CREATE_CHILD_SA para o CGW
AWS resposta processada em túnel (id = xxx) para CREATE_CHILD_SA	AWS recebeu a resposta CREATE_CHILD_SA do CGW

Requisitos do IAM para publicar no CloudWatch Logs

Para que o recurso de log funcione corretamente, a política do IAM anexada à entidade principal do IAM que está sendo usada para configurar o recurso deve incluir, no mínimo, as permissões a seguir. Mais detalhes também podem ser encontrados na seção [Habilitando o registro em determinados AWS serviços](#) do Guia do usuário do Amazon CloudWatch Logs.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "S2SVPNLogging"
    }
  ]
}
```

```
    },
    {
      "Sid": "S2SVPNLoggingCWL",
      "Action": [
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Exibir configuração de logs do Site-to-Site VPN

Como visualizar configurações atuais do registro em log do túnel

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões de VPN de local a local.
3. Selecione a conexão VPN que você deseja visualizar por meio da lista VPN connections (Conexões de VPN).
4. Selecione a guia Tunnel details (Detalhes do túnel).
5. Expanda as seções Tunnel 1 options (Opções de túnel 1) e Tunnel 2 options (Opções de túnel 2) para visualizar todos os detalhes de configuração do túnel.
6. Você pode ver o status atual do recurso de registro em Registro do Tunnel VPN e o grupo de CloudWatch registros atualmente configurado (se houver) em Grupo de CloudWatch registros.

Para visualizar as configurações atuais de registro de túneis em uma conexão VPN Site-to-Site usando a linha de comando ou a API AWS

- [DescribeVpnConnections](#) (API de consulta do Amazon EC2)
- [describe-vpn-connections](#) (AWS CLI)

Habilitar os logs do Site-to-Site VPN

Note

Quando você habilita os logs do Site-to-Site VPN para um túnel de conexão VPN existente, a conectividade por esse túnel pode ser interrompida por vários minutos. No entanto, cada conexão VPN oferece dois túneis para alta disponibilidade, a fim de que você possa ativar o registro em log em um túnel por vez e manter a conectividade pelo túnel inalterada. Para ter mais informações, consulte [Substituições de endpoint de túnel Site-to-Site VPN](#).

Como habilitar o log do Site-to-Site VPN durante a criação de uma conexão do Site-to-Site VPN

Siga o procedimento do [Etapa 5: criar uma conexão VPN](#). Durante a Etapa 9 Tunnel Options (Opções de túnel), você pode especificar todas as opções que deseja usar para ambos os túneis, incluindo as opções de VPN logging (Registro em log de VPN). Para obter mais informações sobre essas opções, consulte [Opções de túnel para a conexão do Site-to-Site VPN](#).

Para habilitar o registro de túneis em uma nova conexão VPN Site-to-Site usando a linha de comando ou a API AWS

- [CreateVpnConnection](#) (API de consulta do Amazon EC2)
- [create-vpn-connection](#) (AWS CLI)

Como habilitar o registro em log do túnel em uma conexão existente do Site-to-Site VPN

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões de VPN de local a local.
3. Selecione a conexão VPN que você deseja modificar por meio da lista VPN connections (Conexões de VPN).
4. Selecione Actions (Ações), Modify VPN tunnel options (Modificar opções de túnel VPN).
5. Selecione o túnel que você deseja modificar escolhendo o endereço IP apropriado na lista VPN tunnel outside IP address (Endereço IP externo do túnel VPN).
6. Em Tunnel activity log (Log de atividades do túnel), selecione Enable (Habilitar).
7. Em Grupo de CloudWatch registros da Amazon, selecione o grupo de CloudWatch registros da Amazon para o qual você deseja que os registros sejam enviados.

8. (Opcional) Em Output format (Formato de saída), escolha o formato desejado para a saída do log, json ou texto.
9. Selecione Save Changes (Salvar alterações).
10. (Opcional) Repita as etapas de 4 a 9 para o outro túnel, se desejar.

Para habilitar o registro de túneis em uma conexão VPN Site-to-Site existente usando a linha de comando ou a API AWS

- [ModifyVpnTunnelOptions](#)(API de consulta do Amazon EC2)
- [modify-vpn-tunnel-options](#) (AWS CLI)

Desabilitar logs do Site-to-Site VPN

Como habilitar o registro em log do túnel em uma conexão do Site-to-Site VPN

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, selecione Conexões de VPN de local a local.
3. Selecione a conexão VPN que você deseja modificar por meio da lista VPN connections (Conexões de VPN).
4. Selecione Actions (Ações), Modify VPN tunnel options (Modificar opções de túnel VPN).
5. Selecione o túnel que você deseja modificar escolhendo o endereço IP apropriado na lista VPN tunnel outside IP address (Endereço IP externo do túnel VPN).
6. Em Tunnel activity log (Log de atividades do túnel), desmarque Enable (Habilitar).
7. Selecione Save Changes (Salvar alterações).
8. (Opcional) Repita as etapas de 4 a 7 para o outro túnel, se desejar.

Para desativar o registro de túneis em uma conexão VPN Site-to-Site usando a linha de comando ou a API AWS

- [ModifyVpnTunnelOptions](#)(API de consulta do Amazon EC2)
- [modify-vpn-tunnel-options](#) (AWS CLI)

Monitoramento de túneis VPN usando a Amazon CloudWatch

Você pode monitorar túneis VPN usando CloudWatch, que coleta e processa dados brutos do serviço VPN em métricas legíveis e quase em tempo real. Essas estatísticas são registradas para um período de 15 meses, de forma que você possa acessar informações históricas e ganhar uma perspectiva melhor sobre como seu serviço ou aplicação Web está se saindo. Os dados métricos da VPN são enviados automaticamente CloudWatch assim que ficam disponíveis.

Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).

Conteúdo

- [Métricas e dimensões da VPN](#)
- [Visualizando CloudWatch métricas de VPN](#)
- [Criação de CloudWatch alarmes para monitorar túneis VPN](#)

Métricas e dimensões da VPN

As CloudWatch métricas a seguir estão disponíveis para suas conexões VPN Site-to-Site.

Métrica	Descrição
TunnelState	<p>O estado dos túneis. Para VPNs estáticos, 0 indica DOWN (INATIVO) e 1 indica UP (ATIVO). Para VPNs BGP, 1 indica ESTABLISHED (ESTABELECIDO) e 0 é usado para todos os outros estados. Para os dois tipos de VPNs, os valores entre 0 e 1 indicam que pelo menos um túnel não está ATIVO.</p> <p>Unidades: valor fracionário entre 0 e 1</p>
TunnelDataIn †	<p>Os bytes recebidos no AWS lado da conexão por meio do túnel VPN de um gateway do cliente. Cada ponto de dados da métrica representa o número de bytes recebidos após o ponto de dados anterior. Use a estatística</p>

Métrica	Descrição
	<p>de soma para mostrar o número total de bytes recebidos durante o período.</p> <p>Essa métrica conta os dados após a descrição da grafia.</p> <p>Unidade: bytes</p>
TunnelDataOut †	<p>Os bytes enviados do AWS lado da conexão pelo túnel VPN até o gateway do cliente. Cada ponto de dados da métrica representa o número de bytes enviados após o ponto de dados anterior. Use a estatística de soma para mostrar o número total de bytes enviados durante o período.</p> <p>Essa métrica conta os dados antes da criptografia.</p> <p>Unidade: bytes</p>

† Essas métricas podem relatar o uso da rede mesmo quando o túnel está inativo. Isso se deve a verificações periódicas de status realizadas no túnel e solicitações ARP e BGP em segundo plano.

Para filtrar os dados das métricas, use as dimensões a seguir.

Dimensão	Descrição
VpnId	Filtra os dados da métrica pelo ID da conexão do Site-to-Site VPN.
TunnelIpAddress	Filtra os dados da métrica pelo endereço IP do túnel para o gateway privado virtual.

Visualizando CloudWatch métricas de VPN

Quando você cria uma conexão VPN Site-to-Site, o serviço VPN envia métricas sobre sua conexão VPN CloudWatch à medida que elas se tornam disponíveis. É possível ver as métricas da conexão VPN da maneira a seguir.

Para visualizar métricas usando o CloudWatch console

As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, por várias combinações de dimensão dentro de cada namespace.

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Métricas.
3. Em All metrics, escolha o namespace de métrica VPN.
4. Selecione a dimensão da métrica para exibir as métricas (por exemplo, Métricas do túnel VPN).

Note

O namespace VPN não aparecerá no CloudWatch console até que uma conexão VPN Site-to-Site tenha sido criada na região que você está visualizando. AWS

Para visualizar métricas usando o AWS CLI

Em um prompt de comando, use o seguinte comando:

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

Criação de CloudWatch alarmes para monitorar túneis VPN

Você pode criar um CloudWatch alarme que envia uma mensagem do Amazon SNS quando o alarme muda de estado. Um alarme observa uma única métrica por um período especificado por você e envia uma notificação para um tópico do Amazon SNS com base no valor da métrica em relação a determinado limite ao longo de vários períodos.

Por exemplo, é possível criar um alarme que monitora o estado de um único túnel VPN e envia uma notificação quando o estado do túnel fica INATIVO para 3 pontos de dados em 15 minutos.

Como criar um alarme para o estado de um único túnel

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, escolha Alarmes e Todos os alarmes.
3. Escolha Criar alarme e Selecionar métrica.
4. Escolha VPN e Métricas do túnel VPN.
5. Selecione o endereço IP do túnel desejado, na mesma linha da TunnelState métrica. Escolha Selecionar métrica.
6. For Whenever TunnelState is... , selecione Inferior e, em seguida, digite "1" no campo de entrada abaixo de... .
7. Em Configuração adicional, defina as entradas como "3 de 3" em Pontos de dados a acionar.
8. Escolha Próximo.
9. Em Enviar uma notificação ao seguinte tópico do SNS, selecione uma lista de notificações existente ou crie uma.
10. Escolha Próximo.
11. Insira um nome para o alarme. Escolha Próximo.
12. Verifique as configurações do alarme e, depois, escolha Create alarm (Criar alarme).

Você pode criar um alarme que monitore o estado da conexão do Site-to-Site VPN. Por exemplo, é possível criar um alarme que envie uma notificação quando o status de um ou de ambos os túneis estiver INATIVO por um período de 5 minutos.

Para criar um alarme para o estado da conexão do Site-to-Site VPN

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, escolha Alarmes e Todos os alarmes.
3. Escolha Criar alarme e Selecionar métrica.
4. Escolha VPN e VPN Connection Metrics (Métricas de conexão VPN).
5. Selecione sua conexão VPN Site-to-Site e a métrica. TunnelState Escolha Select metric (Selecionar métrica).
6. Em Statistic (Estatística), especifique Maximum (Máximo).

Como alternativa, se você configurou sua conexão do Site-to-Site VPN para que ambos os túneis sejam ativados, você pode especificar uma estatística Minimum (Mínimo) para enviar uma notificação quando pelo menos um túnel estiver desativado.

7. Em Whenever (Sempre que), escolha Lower/Equal (Abaixo de/igual a) (\leq) e insira 0 (ou 0,5 para quando pelo menos um túnel estiver inativo). Escolha Próximo.
8. Em Select an SNS topic (Selecionar um tópico do SNS), selecione uma lista de notificações existente ou escolha New list (Nova lista) para criar uma nova. Escolha Próximo.
9. Insira um nome e uma descrição para o alarme. Escolha Próximo.
10. Verifique as configurações do alarme e, depois, escolha Create alarm (Criar alarme).

Além disso, você pode criar alarmes que monitoram a quantidade de tráfego que está entrando ou saindo de um túnel VPN. Por exemplo, o alarme a seguir monitora a quantidade de tráfego de sua rede que está entrando no túnel VPN e envia uma notificação quando o número de bytes atingir o limite de 5.000.000 durante o período de 15 minutos.

Para criar um alarme para tráfego de rede de entrada

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, escolha Alarmes e Todos os alarmes.
3. Escolha Criar alarme e Selecionar métrica.
4. Escolha VPN e VPN Tunnel Metrics (Métricas de túnel VPN).
5. Selecione o endereço IP do túnel VPN e a TunnelDataInmétrica. Escolha Select metric (Selecionar métrica).
6. Em Statistic (Estatística), especifique Sum (Soma).
7. Em Period (Período), selecione 15 minutes (15 minutos).
8. Em Whenever (Sempre que), escolha Greater/Equal (Maior que/igual a) (\geq) e insira 5000000. Escolha Próximo.
9. Em Select an SNS topic (Selecionar um tópico do SNS), selecione uma lista de notificações existente ou escolha New list (Nova lista) para criar uma nova. Escolha Próximo.
10. Insira um nome e uma descrição para o alarme. Escolha Próximo.
11. Verifique as configurações do alarme e, depois, escolha Create alarm (Criar alarme).

O alarme a seguir monitora a quantidade de tráfego de sua rede que está saindo do túnel VPN e envia uma notificação quando o número de bytes for inferior a 1.000.000 durante o período de 15 minutos.

Para criar um alarme para tráfego de rede de saída

1. Abra o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, escolha Alarmes e Todos os alarmes.
3. Escolha Criar alarme e Selecionar métrica.
4. Escolha VPN e VPN Tunnel Metrics (Métricas de túnel VPN).
5. Selecione o endereço IP do túnel VPN e a TunnelDataOutmétrica. Escolha Select metric (Selecionar métrica).
6. Em Statistic (Estatística), especifique Sum (Soma).
7. Em Period (Período), selecione 15 minutes (15 minutos).
8. Em Whenever (Sempre que), escolha Lower/Equal (Inferior/igual) (\leq) e insira 1000000. Escolha Próximo.
9. Em Select an SNS topic (Selecionar um tópico do SNS), selecione uma lista de notificações existente ou escolha New list (Nova lista) para criar uma nova. Escolha Próximo.
10. Insira um nome e uma descrição para o alarme. Escolha Próximo.
11. Verifique as configurações do alarme e, depois, escolha Create alarm (Criar alarme).

Para obter mais exemplos de criação de alarmes, consulte [Criação de CloudWatch alarmes da Amazon](#) no Guia CloudWatch do usuário da Amazon.

Monitoramento de conexões VPN usando AWS Health eventos

AWS Site-to-Site VPN envia notificações automaticamente para o AWS [AWS Health Dashboard](#)(PHD), que é alimentado pela AWS Health API. Esse painel não requer configuração e está pronto para ser usado por AWS usuários autenticados. Você pode configurar várias ações em resposta às notificações de eventos por meio do AWS Health Dashboard.

O AWS Health Dashboard fornece os seguintes tipos de notificações para suas conexões VPN:

- [Notificações de substituição de endpoint do túnel](#)
- [Notificações de VPN de túnel único](#)

Notificações de substituição de endpoint do túnel

Você recebe uma notificação de substituição de endpoint de túnel AWS Health Dashboard quando um ou ambos os endpoints de túnel VPN em sua conexão VPN são substituídos. Um endpoint de túnel é substituído quando a AWS executa atualizações de túnel ou quando você modifica a conexão VPN. Para ter mais informações, consulte [Substituições de endpoint de túnel Site-to-Site VPN](#).

Quando uma substituição do endpoint do túnel é concluída, AWS envia a notificação de substituição do endpoint do túnel por meio de um AWS Health Dashboard evento.

Notificações de VPN de túnel único

Uma conexão do Site-to-Site VPN consiste em dois túneis para redundância. É altamente recomendável configurar ambos os túneis para alta disponibilidade. Se sua conexão VPN tiver um túnel ativado e o outro desativado por mais de uma hora em um dia, você receberá uma notificação de túnel único de VPN mensal por meio de um evento AWS Health Dashboard . Esse evento será atualizado diariamente com todas as novas conexões VPN detectadas como um único túnel, com notificações enviadas semanalmente. A cada mês será criado um evento, o que apagará todas as conexões VPN que não forem mais detectadas como um único túnel.

Cotas do Site-to-Site VPN

Sua AWS conta tem as seguintes cotas, anteriormente chamadas de limites, relacionadas à VPN Site-to-Site. A menos que especificado de outra forma, cada cota é específica da região . É possível solicitar aumentos para algumas cotas e outras cotas não podem ser aumentadas.

Para solicitar o aumento da cota para uma cota ajustável, selecione Yes (Sim) na coluna Adjustable (Ajustável). Para obter mais informações, consulte [Solicitar um aumento da cota](#) no Guia do usuário do Service Quotas.

Recursos do Site-to-Site VPN

Nome	Padrão	Ajustável
Gateways do cliente por região	50	Sim
Gateways privados virtuais por região	5	Sim
Conexões de VPN de local a local por região	50	Sim
Conexões de VPN de local a local por gateway privado virtual	10	Sim
Conexões do Site-to-Site VPN aceleradas por região	10	Sim
Conexões desassociadas do Site-to-Site VPN por região	10	Sim

Note

Tanto as conexões aceleradas quanto as desassociadas são incluídas no cálculo da cota total de conexões do Site-to-Site VPN por região.

Um gateway privado virtual pode ser associado a uma VPC de cada vez. Para conectar a mesma conexão do Site-to-Site VPN a várias VPCs, recomendamos que você explore o uso de um gateway

de trânsito. Para obter mais informações, consulte [Gateways de trânsito](#) em Gateways de trânsito da Amazon VPC.

As conexões de VPN de local a local em um gateway de trânsito estão sujeitas ao limite total de anexos do gateway trânsito. Para obter mais informações, consulte [Cotas para os gateways de trânsito](#).

Rotas

As fontes de rota publicadas incluem rotas da VPC, outras rotas da VPN e rotas de interfaces virtuais do AWS Direct Connect . As rotas publicadas vêm da tabela de rotas associada ao anexo da VPN.

Note

Se você estiver usando um gateway privado virtual e a propagação de rotas estiver ativada na tabela de rotas da VPC, as rotas dinâmicas e estáticas serão adicionadas automaticamente à sua conexão VPN, até o limite da tabela de rotas da VPC. Consulte [Cotas da Amazon VPC](#) no Guia do usuário da Amazon VPC para obter mais detalhes.

Nome	Padrão	Ajustável
Rotas dinâmicas publicadas de um dispositivo de gateway do cliente para uma conexão de VPN de local a local em um gateway privado virtual	100	Não
Rotas publicadas de uma conexão de VPN de local a local em um gateway privado virtual para um dispositivo de gateway do cliente	1.000	Não
Rotas dinâmicas publicadas de um dispositivo de gateway do cliente para uma conexão de VPN de local a local em um gateway de trânsito	1.000	Não

Nome	Padrão	Ajustável
Rotas publicadas de uma conexão de VPN de local a local em um gateway de trânsito para um dispositivo de gateway do cliente	5.000	Não
Rotas estáticas de um dispositivo gateway do cliente para uma conexão VPN Site-to-Site em um gateway privado virtual	100	Não

Largura de banda e taxa de transferência

Há muitos fatores que podem afetar a largura de banda realizada por meio de uma conexão Site-to-Site VPN, incluindo, mas não limitado a: tamanho do pacote, combinação de tráfego (TCP/UDP), políticas de controle de utilização em redes intermediárias, clima da Internet e requisitos específicos de aplicações.

Nome	Padrão	Ajustável
Largura de banda máxima por túnel de VPN	Até 1,25 Gbps	Não
Máximo de pacotes por segundo (PPS) por túnel da VPN	Até 140.000	Não

Para conexões do Site-to-Site VPN em um gateway de trânsito, você pode usar ECMP para ter uma largura de banda maior de VPN ao agregar vários túneis da VPN. Para usar o ECMP, a conexão VPN deve ser configurada para roteamento dinâmico. O ECMP não é compatível com conexões VPN que usam roteamento estático. Para obter mais informações, consulte [Gateways de trânsito](#).

A unidade de transmissão máxima (MTU).

Uma VPN Site-to-Site suporta uma unidade de transmissão máxima (MTU) de 1446 bytes e um tamanho máximo de segmento correspondente (MSS) de 1406 bytes. No entanto, certos algoritmos que usam cabeçalhos TCP maiores podem efetivamente reduzir esse valor máximo. Para evitar fragmentação, recomendamos que você configure a MTU e o MSS com base nos algoritmos

selecionados. Para obter mais detalhes sobre MTU, MSS e os valores ótimos, consulte [Práticas recomendadas para o dispositivo de gateway do cliente](#).

Não há suporte para frames jumbo. Para obter mais informações, consulte [Jumbo frames](#) no Guia do usuário do Amazon EC2.

Uma conexão do Site-to-Site VPN não é compatível com a Path MTU Discovery

Recursos de cota adicionais

Para cotas relacionadas a gateways de trânsito, incluindo o número de anexos em um gateway de trânsito, consulte [Cotas para seus gateways de trânsito](#) no Guia dos gateways de trânsito da Amazon VPC.

Para obter as cotas adicionais da VPC, consulte [Cotas da Amazon VPC](#) no Guia do usuário da Amazon VPC.

Histórico do documento do Guia do usuário do Site-to-Site VPN

A tabela a seguir descreve as atualizações AWS Site-to-Site VPN do Guia do usuário.

Alteração	Descrição	Data
Informações sobre a VPN clássica removidas	As informações sobre a VPN clássica foram removidas do guia.	19 de janeiro de 2023
Exemplo de mensagens de log da VPN	Adição de exemplos de log para as conexões do Site-to-Site VPN.	9 de dezembro de 2022
Utilitário de configuração de download atualizado	Os clientes da Site-to-Site VPN podem gerar modelos de configuração para dispositivos CGW (gateway do cliente) compatíveis, facilitando a criação de conexões VPN com a AWS. Esta atualização adiciona suporte aos parâmetros do Internet Key Exchange versão 2 (IKEv2) para muitos dispositivos CGW populares e inclui duas novas APIs — e. <code>GetVpnConnectionDeviceTypes</code> <code>GetVpnConnectionDeviceSampleConfiguration</code>	21 de setembro de 2021
Notificações de conexão VPN	O Site-to-Site VPN envia automaticamente notificações	29 de outubro de 2020

	sobre sua conexão VPN ao AWS Health Dashboard.	
Iniciação do túnel da VPN	Você pode configurar seus túneis VPN para que os AWS túneis apareçam.	27 de agosto de 2020
Modificar opções da conexão VPN	Você pode modificar as opções de conexão para sua conexão do Site-to-Site VPN.	27 de agosto de 2020
Algoritmos de segurança adicionais	É possível aplicar algoritmos de segurança adicionais aos túneis VPN.	14 de agosto de 2020
Suporte a IPv6	Seus túneis VPN podem oferecer suporte ao tráfego IPv6 dentro dos túneis.	12 de agosto de 2020
Guias de mesclagem AWS Site-to-Site VPN	Esta versão mescla o conteúdo do Guia do Administrador de AWS Site-to-Site VPN Rede com este guia.	31 de março de 2020
Conexões aceleradas AWS Site-to-Site VPN	Você pode ativar a aceleração para sua AWS Site-to-Site VPN conexão.	3 de dezembro de 2019
Modificar opções de AWS Site-to-Site VPN túnel	Você pode modificar as opções de um túnel VPN em uma AWS Site-to-Site VPN conexão. Também é possível configurar opções de túnel adicionais.	29 de agosto de 2019
AWS Private Certificate Authority suporte a certificados privados	Você pode usar um certificado privado de AWS Private Certificate Authority para autenticar sua VPN.	15 de agosto de 2019

Novo guia do usuário do Site-to-Site VPN	Esta versão separa o conteúdo AWS Site-to-Site VPN (anteriormente conhecido como VPN AWS gerenciada) do Guia do usuário da Amazon VPC.	18 de dezembro de 2018
Modificar o gateway de destino	Você pode modificar o gateway de destino da AWS Site-to-Site VPN conexão.	18 de dezembro de 2018
ASN personalizado	Quando você cria um gateway privado virtual, é possível especificar o Número de sistema autônomo privado (ASN) para o lado da Amazon do gateway.	10 de outubro de 2017
Opções de túnel VPN	Você pode especificar blocos CIDR de túnel e personalizar as chaves pré-compartilhadas para seus túneis VPN.	3 de outubro de 2017
Métricas da VPN	Você pode ver CloudWatch as métricas de suas conexões VPN.	15 de maio de 2017

[Melhorias do VPN](#)

Uma conexão VPN agora oferece suporte à função de criptografia AES de 256 bits, função hashing SHA-256, NAT transversal e outros grupos Diffie-Hellman durante a Fase 1 e a Fase 2 de uma conexão. Além disso, agora você pode usar o mesmo endereço IP do gateway do cliente para cada conexão VPN que usa o mesmo dispositivo de gateway do cliente.

28 de outubro de 2015

[Conexões VPN usando configuração de roteamento estático](#)

Você pode criar conexões VPN IPsec para a Amazon VPC usando configurações de roteamento estático. Anteriormente, as conexões VPN exigiam o uso do protocolo de gateway de borda (BGP). Agora damos suporte a ambos os tipos de conexões e você pode estabelecer conectividade de dispositivos que não oferece suporte ao BGP, incluindo Cisco ASA e Microsoft Windows Server 2008 R2.

13 de setembro de 2012

[Propagação automática de rotas](#)

Agora você pode configurar a propagação automática de rotas de sua VPN e AWS Direct Connect links para suas tabelas de roteamento de VPC.

13 de setembro de 2012

[AWS VPN CloudHub e conexões VPN redundantes](#)

Você pode se comunicar seguramente de um local para outro com ou sem uma VPC. É possível usar conexões VPN redundantes para oferecer à sua VPC uma conexão tolerante a falhas.

29 de setembro de 2011

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.